
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA STROJNÍHO INŽENÝRSTVÍ
FACULTY OF MECHANICAL ENGINEERING

## ÚSTAV VÝROBNÍCH STROJŮ, SYSTÉMŮ A ROBOTIKY
INSTITUTE OF PRODUCTION MACHINES, SYSTEMS AND ROBOTICS


# ZLEPŠENÍ PODNIKOVÝCH PROCESŮ ZAJIŠŤOVÁNÍ BEZPEČNOSTI PRODUKTŮ
IMPROVEMENT OF COMPANY PROCESSES TO ASSURE SAFETY OF PRODUCTS

**DIPLOMOVÁ PRÁCE**
MASTER'S THESIS


**AUTOR PRÁCE** — **Bc. Kateřina Zvolánková**
AUTHOR

**VEDOUCÍ PRÁCE** — **doc. Dr. Ing. Daniel Prostředník, CSc.**
SUPERVISOR



**BRNO 2020**

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA STROJNÍHO INŽENÝRSTVÍ

# Zadání diplomové práce

| | |
|---|---|
| Ústav: | Ústav výrobních strojů, systémů a robotiky |
| Studentka: | **Bc. Kateřina Zvolánková** |
| Studijní program: | Strojní inženýrství |
| Studijní obor: | Kvalita, spolehlivost a bezpečnost |
| Vedoucí práce: | **doc. Dr. Ing. Daniel Prostredník, CSc.** |
| Akademický rok: | 2019/20 |

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

## Zlepšení podnikových procesů zajišťování bezpečnosti produktů

**Stručná charakteristika problematiky úkolu:**

Hlavním úkolem diplomové práce, je popis postupu při řešení projektů na úrovni jednotlivých kroků, které musí být provedeny pro dosažení požadovaného stupně funkční bezpečnosti produktů. Pro úspěšné vyřešení zadaných cílů je potřeba věnovat pozornost teoretické přípravě, ve které bude rozebraný stav problematiky v ČR, EU s důrazem na platné harmonizované normy a směrnice EU včetně zdůvodnění vybraných postupů pro zajištění funkční bezpečnosti produktů. Práce je řešená na VUT Brno ve spolupráci, resp. se souhlasem firmy Bosch Rexroth.

**Cíle diplomové práce:**

Rešerše aktuálního stavu vědy a techniky v oblasti bezpečnosti produktů.
Popis aktuálního stavu v oblasti funkční bezpečnosti produktů v Bosch Rexroth.
Popis vhodných standardů a metod pro zajištění funkční bezpečnosti produktů se zaměřením na projekty.
Návrh na zlepšení funkční bezpečnosti produktů se zaměřením na zvolenou podskupinu lisu na úrovni bloků.
Implementace vybraných postupů zajišťování funkční bezpečnosti produktů v rámci organizace.
Vlastní závěry a doporučení pro praxi.

**Seznam doporučené literatury:**

STERRER, C., and G. WINKLER. Let your projects fly. Wien: Goldegg Verlag, 2006, ISBN 10 3-901880-67-4.

DRÖSCHEL, W. and M. WIEMERS. Das V-Modell 97. München: Oldenbourg Verlag, 2000.

SVOZILOVÁ, A. Projektový management. Praha: Grada, 2006. ISBN 80-247-1501-5.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně, dne

L. S.

| | |
|---|---|
| doc. Ing. Petr Blecha, Ph.D.<br>ředitel ústavu | doc. Ing. Jaroslav Katolický, Ph.D.<br>děkan fakulty |

# ABSTRAKT

Diplomová práce se věnuje procesu zajišťování funkční bezpečnosti u produktů brněnské společnosti Bosch Rexroth, jež se zabývá průmyslovými hydraulickými systémy. V první části jsou představeny základní legislativní předpisy týkající se bezpečnosti produktů a dále jsou zde popsány vybrané normy relevantní pro tuto práci. Druhá část se zaměřuje na společnost Bosch Rexroth a na aktuální stav v oblasti zajišťování funkční bezpečnosti u jejich produktů. Součástí je také popis řešení funkční bezpečnosti na konkrétním projektu – hydraulickém zapracovávacím lisu. V závěru práce jsou navrhnuta zlepšení procesu zajišťování funkční bezpečnosti reagující na zjištěné nedostatky.



# ABSTRACT

The diploma thesis devotes to the process of ensuring functional safety of products in Bosch Rexroth Brno, which deals with industrial hydraulic systems. The first part introduces the basic legislative regulations concerning product safety and describes selected standards relevant to this thesis. The second part focuses on Bosch Rexroth and the current state in the field of ensuring functional safety of their products. It also includes a description of the functional safety solution of a specific project – a hydraulic try-out press. At the end of the thesis, improvements to the process of ensuring functional safety in response to the identified shortcomings are proposed.



# KLÍČOVÁ SLOVA

Bezpečnost produktů, funkční bezpečnost, bezpečnostní funkce, úroveň vlastností, projekty, hydraulický zapracovávací lis

# KEYWORDS

Product safety, functional safety, safety function, performance level, projects, hydraulic try-out press

# BIBLIOGRAFICKÁ CITACE

ZVOLÁNKOVÁ, K. *Zlepšení podnikových procesů zajišťování bezpečnosti produktů,* Brno, Vysoké učení technické v Brně, Fakulta strojního inženýrství. 2020, 89 s., Vedoucí diplomové práce doc. Dr. Ing. Daniel Prostredník, CSc.

# PODĚKOVÁNÍ

Tímto bych chtěla poděkovat doc. Dr. Ing. Danielu Prostredníkovi, CSc. a zaměstnancům brněnské společnosti Bosch Rexroth za trpělivost, ochotu, pomoc a cenné rady při zpracování této práce. Rovněž bych chtěla poděkovat své rodině a blízkým za podporu při studiích.

# ČESTNÉ PROHLÁŠ ENÍ

Prohlašuji, že tato práce je mým původním dílem, zpracovala jsem ji samostatně pod vedením doc. Dr. Ing. Daniela Prostredníka, CSc. a s použitím literatury uvedené v seznamu.

V Brně dne 23. 6. 2020 ……

Kateřina Zvolánková

# OBSAH

# 1 ÚVOD

Základním požadavkem týkajícím se strojních zařízení je jejich bezpečnost. Za účelem zajištění optimální dosažitelné úrovně bezpečnosti vzniklo mnoho předpisů a norem definující různé metody a postupy, ale ani s jejich pomocí nelze nikdy eliminovat všechna rizika spojená s daným zařízením. Lze je však alespoň snížit na přijatelnou úroveň.

V souvislosti s rozvojem automatizace jsou již nedílnou součástí mnoha strojních zařízení ovládací systémy, jež mohou přispívat ke snížení rizik vykonáváním bezpečnostních funkcí, a podílet se tak na celkové bezpečnosti zařízení. Aby tyto systémy vykonávaly svoji funkci správně, je nutné se zabývat funkční bezpečností.

Funkční bezpečnost není důležitá pouze z pohledu bezpečnosti osob, ale také z pohledu ochrany životního prostředí a majetku. Spousta výrobců však funkční bezpečnosti z různých důvodů nevěnuje patřičnou pozornost, a riskují tak nemalé postihy spojené s nedodržením legislativních požadavků a v krajním případě také s úrazy způsobenými nebezpečným zařízením.

Tato diplomová práce se zabývá návrhem na zlepšení procesů zajišťování funkční bezpečnosti v brněnské společnosti Bosch Rexroth. Vzhledem k obsáhlosti tohoto tématu je součástí práce řešení funkční bezpečnosti pouze u hardwaru.

Úvodní část je věnována popisu základních legislativních požadavků týkajících se bezpečnosti, a to jak z pohledu Evropské unie, tak i České republiky. Na tuto část navazuje také popis vybraných norem, které jsou z pohledu této práce důležité. Jsou zde popsány nejenom stěžejní normy týkající se funkční bezpečnosti (konkrétně ČSN EN 61508, ČSN EN ISO 13849 a ČSN EN 62061), ale také norma ČSN EN ISO 12100, jež se zabývá posouzením a snížením rizik jakožto velice důležitou částí pro zajištění požadované úrovně funkční bezpečnosti, a norma ISO 16092 popisující požadavky na bezpečnost lisů, protože požadavky v ní uvedené budou dále využity při řešení funkční bezpečnosti u konkrétního projektu.

Další část diplomové práce je věnována společnosti Bosch Rexroth a zajišťování funkční bezpečnosti u jejich produktů, které lze rozdělit do tří skupin: hydraulické komponenty, hydraulické agregáty a projekty. Funkční bezpečnost je aktivně řešena v rámci brněnské pobočky hlavně u projektů, a proto bude zbytek práce zaměřen právě na zlepšení procesu zajišťování funkční bezpečnosti v této oblasti.

Aby bylo možné navrhnout zlepšení „na míru“, je součástí práce také popis, jakým způsobem jsou aktuálně projekty řešeny. Pro lepší pochopení celé problematiky zajišťování funkční bezpečnosti je postup dle normy ČSN EN ISO 13849, která je vzhledem k povaze produktů nejlépe aplikovatelná, ukázán na reálném projektu. Pro účely této práce byl vybrán zapracovávací (zkušební) lis, jež je využíván pro zkoušení nástrojů (forem) určených k lisování částí karoserií automobilů.

S využitím získaných informací je v poslední a nejdůležitější části z pohledu přínosu pro společnost popsán samotný návrh na zlepšení procesu zajišťování funkční bezpečnosti.

# 2 LEGISLATIVA V OBLASTI BEZPEČNOSTI PRODUKTŮ

Bezpečnost je jedním z klíčových znaků kvality produktu, který je vyžadován nejenom zákazníky, ale hlavně legislativními předpisy. Za účelem ochrany spotřebitele před nebezpečnými výrobky bylo vydáno mnoho předpisů stanovujících požadavky na bezpečnost, jež musí být při uvádění výrobků na trh splněny. Tato kapitola uvádí pouze nejdůležitější z nich.

## 2.1 Obecná bezpečnost výrobků

Základem bezpečnosti výrobků dodávaných na trh v rámci Evropské unie je směrnice Evropského parlamentu a Rady 2001/95/ES o obecné bezpečnosti výrobků. Tato směrnice vznikla za účelem zajistit, že na trh budou dodávány pouze výrobky, které jsou bezpečné. To znamená výrobky, které „*za běžných nebo rozumně předvídatelných podmínek použití, včetně požadavků na životnost, a případně na uvedení do provozu, instalaci a údržbu, nepředstavují žádné riziko nebo představují pouze minimální rizika slučitelná s použitím výrobku a považovaná za přijatelná a odpovídající vysoké úrovni ochrany zdraví a bezpečnosti osob.*“ Při posuzování bezpečnosti výrobku je přihlíženo např. k jeho vlastnostem, složení, dostupnosti a srozumitelnosti návodů, vlivu na jiné výrobky aj. Výrobek je bezpečný v případě splnění požadavků daných evropskými nebo vnitrostátními předpisy. Pokud takové předpisy neexistují, jsou používány jiné dokumenty, např. normy. [1]

Výrobci jsou povinni informovat o nebezpečích spojených s výrobky a v případě nutnosti musí zajistit, že nedojde k újmě, např. stažením výrobku z trhu, upozorněním uživatelů atd. Každý výrobek musí být označen údaji o výrobci a jedinečným identifikačním číslem, aby bylo možné později vysledovat případné nebezpečné výrobky. Pro předávání informací o nebezpečných výrobcích byl zaveden systém Evropské unie pro rychlou výměnu informací RAPEX (Rapid Alert System for Non-Food Products), který se však nevztahuje na potraviny, léčiva a zdravotnické prostředky. Oznámení nebezpečného výrobku musí obsahovat informace potřebné pro identifikaci výrobku, popis nebezpečí a informace nutné pro posouzení úrovně rizika, dále informace o opatřeních a informace týkající se distribuce výrobku. [1]

Výše zmíněná směrnice Evropského parlamentu a Rady 2001/95/ES o obecné bezpečnosti výrobků je v České republice implementována v podobě zákona č. 102/2001 Sb.

## 2.2 Nový legislativní rámec

Nový legislativní rámec byl vytvořen za účelem zvýšení bezpečnosti občanů a zjednodušení volného pohybu výrobků v rámci jednotného trhu. Zahrnuje všechny části, jimiž je nutné se zabývat v rámci zajištění bezpečnosti výrobků, a může být využit ve všech oblastech. Je tvořen třemi právními dokumenty. [2]

Prvním dokumentem je nařízení Evropského parlamentu a Rady č. 764/2008/ES stanovující postupy, jež se týkají uplatňování některých vnitrostátních technických pravidel u výrobků uvedených na trh v souladu s právními předpisy v jiném členském státě (tzv. nařízení o vzájemném uznávání).

Je založeno na předpokladu, že výrobek, který splňuje požadavky jednoho členského státu, a byl tak legálně uveden na jeho trh, může být dodáván i do ostatních členských států.

Jinak řečeno: co je bezpečné pro občany jednoho státu, to nepředstavuje nebezpečí pro občany jiných států. Tento dokument bude nahrazen s účinností od 19. 4. 2020 nařízením Evropského parlamentu a Rady č. 2019/515/EU. [2]

Dalším dokumentem je nařízení Evropského parlamentu a Rady 765/2008/ES, které stanovuje požadavky na akreditaci a dozor nad trhem při uvádění výrobků na trh. Cílem je určit rámec pro to, aby výrobky plnily požadavky týkající se vysoké úrovně ochrany zdraví a také životního prostředí. Definuje i pravidla pro organizaci a provádění akreditací subjektů pro posuzování shody, obecné zásady pro označení CE a rámec pro kontroly výrobků ze třetích zemí. [2]

Poslední je rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES o společném rámci pro uvádění výrobků na trh popisující postupy posuzování shody, definice a povinnosti hospodářských subjektů, pravidla pro označení CE a požadavky na subjekty posuzování shody. Na tento předpis navazují další předpisy Evropské unie zabývající se konkrétními typy výrobků, např. směrnice Evropského parlamentu a Rady 2014/68/EU o harmonizaci právních předpisů členských států týkajících se dodávání tlakových zařízení na trh či směrnice Evropského parlamentu a Rady 2014/30/EU o harmonizaci právních předpisů členských států týkajících se elektromagnetické kompatibility. [2]

*Implementace nového legislativního rámce v ČR*

V České republice je nový legislativní rámec implementován hlavně v podobě zákona č. 22/1997 Sb. o technických požadavcích na výrobky a zákona č. 90/2016 o posuzování shody stanovených výrobků při jejich dodávání na trh.

Zákon č. 22/1997 Sb. se zabývá požadavky na výrobky, které mohou ve vyšší míře představovat nebezpečí pro zdraví, majetek či životní prostředí (tzv. stanovené výrobky), právy a povinnostmi osob, které dodávají tyto výrobky na trh, distribuují je či uvádějí do provozu, a také reguluje tvorbu a uplatňování českých technických norem a státní zkušebnictví. [3]

U stanovených výrobků musí být dle zákona č. 90/2016 Sb. posouzena shoda se specifikovanými požadavky. Požadavky pro konkrétní typy výrobků jsou uvedeny v navazujících nařízeních vlády, např. nařízení vlády č. 219/2016 o posuzování shody tlakových zařízení při jejich dodávání na trh, jež vychází z již zmíněné směrnice Evropského parlamentu a Rady 2014/68/EU. Nařízení vlády kromě technických požadavků obsahují také způsoby posuzování shody s využitím modulů shody, podmínky a pravidla pro vypracování EU (ES) prohlášení o shodě, podobu a způsob označení shody (nejčastěji CE), postupy při dodávání výrobků na trh a podrobnosti k činnostem subjektů při posuzování shody. Pokud výrobek nesplňuje dané požadavky a nebylo vydáno prohlášení o shodě, nesmí být uveden na trh. [4]

Pro výrobky, které nespadají do regulované sféry (nestanovené výrobky), platí zákon č. 102/2001 Sb. o obecné bezpečnosti výrobků a nemusí u nich být provedeno posouzení shody.

## 2.3 Bezpečnost strojních zařízení

Strojní zařízení je definováno jako [5]:

- *„soubor, který je vybaven nebo má být vybaven poháněcím systémem, který nepoužívá přímo vynaloženou lidskou nebo zvířecí sílu, sestavený z částí nebo součástí, z nichž alespoň jedna je pohyblivá, vzájemně spojených za účelem přesně stanoveného použití,*
- *soubor uvedený v první odrážce, kterému chybí pouze ty součásti, které jej spojují s místem použití nebo se zdroji energie či pohybu,*
- *soubor uvedený v první nebo druhé odrážce, který je připraven k instalaci a je schopen fungovat až po namontování na dopravní prostředek nebo po instalaci v budově nebo na konstrukci,*
- *soubory strojních zařízení uvedené v první, druhé nebo třetí odrážce nebo neúplná strojní zařízení, které jsou za účelem dosažení stejného výsledku uspořádány a ovládány tak, aby pracovaly jako integrovaný celek,*
- *soubor spojených částí nebo součástí, z nichž alespoň jedna je pohyblivá, které jsou vzájemně spojeny za účelem zvedání břemen a jejichž jediným zdrojem energie je přímo vynaložená lidská síla.“*

Strojní zařízení patří mezi stanovené výrobky a vztahuje se na ně zvláštní předpis. Tím je směrnice Evropského parlamentu a Rady 2006/42/ES. Vztahuje se nejenom na strojní zařízení, ale také na vyměnitelná přídavná zařízení, bezpečnostní součásti, příslušenství pro zdvihání, řetězy, lana a popruhy, snímatelná mechanická převodová zařízení a neúplná strojní zařízení. Předmětem předpisu je stanovení základních požadavků na ochranu zdraví a bezpečnost, přičemž jsou zde uvedeny také zvláštní předpisy týkající se některých konkrétních druhů nebezpečí. Kromě toho popisuje i podmínky pro uvedení strojních zařízení na trh nebo do provozu, postupy posuzování shody aj. [5]

Směrnice Evropského parlamentu a Rady 2006/42/ES je v České republice zavedena v podobě nařízení vlády č. 176/2008 o technických požadavcích na strojní zařízení.

Na strojní zařízení se mohou vztahovat také další předpisy. Příkladem může být:

- **směrnice Evropského parlamentu a Rady 2014/30/EU** o harmonizaci právních předpisů členských států týkajících se elektromagnetické kompatibility (v České republice implementováno jako nařízení vlády č. 117/2016 Sb.)
- **směrnice Evropského parlamentu a Rady 2014/35/EU** o harmonizaci právních předpisů členských států týkajících se dodávání elektrických zařízení určených pro používání v určitých mezích napětí na trh (v České republice implementováno jako nařízení vlády č. 118/2016 Sb.)

*Harmonizované normy*

Harmonizované normy slouží jako podpora při implementaci legislativních požadavků na strojní zařízení do praxe. Splnění požadavků uvedených v harmonizovaných normách není povinné, ale pokud jsou splněny, předpokládá se i splnění požadavků příslušného evropského předpisu. [7]

V oblasti bezpečnosti strojních zařízení jsou rozlišovány 3 druhy norem [6]:

- **Normy typu A (základní bezpečnostní normy)**
  Tyto normy definují základní pojmy, zásady pro konstrukci a univerzální stanoviska, které je možné využít u všech strojních zařízení. Jsou také stěžejní pro tvorbu norem typu B a C.

  Příklady norem typu A:
  - ČSN EN ISO 12100
    Bezpečnost strojních zařízení – Všeobecné zásady pro konstrukci – Posouzení rizika a snižování rizika

- **Normy typu B (skupinové bezpečnostní normy)**
  Zabývají se buď jedním konkrétním bezpečnostním aspektem (typ B1), např. hlukem či bezpečnými vzdálenostmi, nebo jedním konkrétním bezpečnostním zařízením (typ B2), např. ochrannými kryty, dvouručním ovládáním atd.

  Příklady norem typu B1:
  - ČSN EN ISO 13849-1
    Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 1: Obecné zásady pro konstrukci,
  - ČSN EN 61508-1 ed. 2
    Funkční bezpečnost elektrických/elektronický/programovatelných elektronických systémů souvisejících s bezpečností – Část 1: Všeobecné požadavky,
  - ČSN EN 60204-1 ed. 3
    Bezpečnost strojních zařízení – Elektrická zařízení strojů – Část 1: Obecné požadavky.

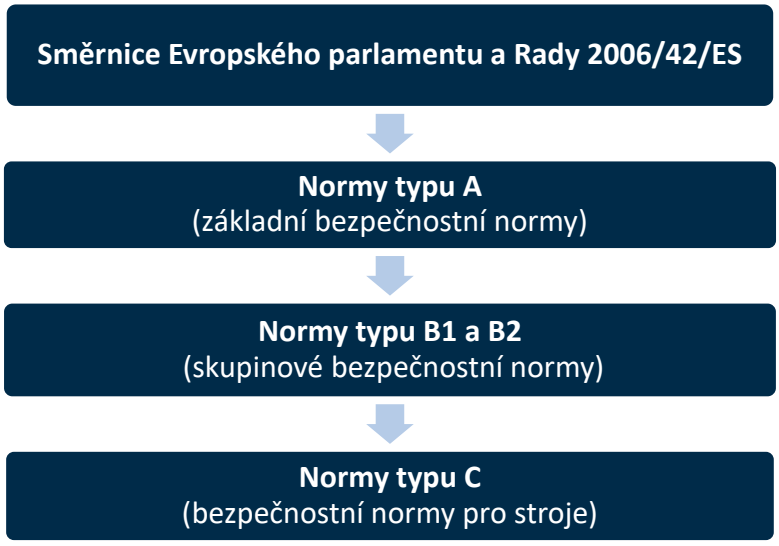
  Příklady norem typu B2:
  - ČSN EN ISO 13850
    Bezpečnost strojních zařízení – Funkce nouzového zastavení – Zásady pro konstrukci
  - ČSN EN ISO 14119
    Bezpečnost strojních zařízení – Blokovací zařízení spojená s ochrannými kryty – Zásady pro konstrukci a volbu

- **Normy typu C (bezpečnostní normy pro stroje)**
  Týkají se požadavků na bezpečnost konkrétního stroje nebo skupiny strojů.

  Příklady norem typu C:
  - ČSN EN ISO 10218-1
    Roboty a robotická zařízení – Požadavky na bezpečnost průmyslových robotů – Část 1: Roboty
  - ČSN EN ISO 16092-1
    Bezpečnost obráběcích a tvářecích strojů – Lisy – Část 1: Obecné bezpečnostní požadavky

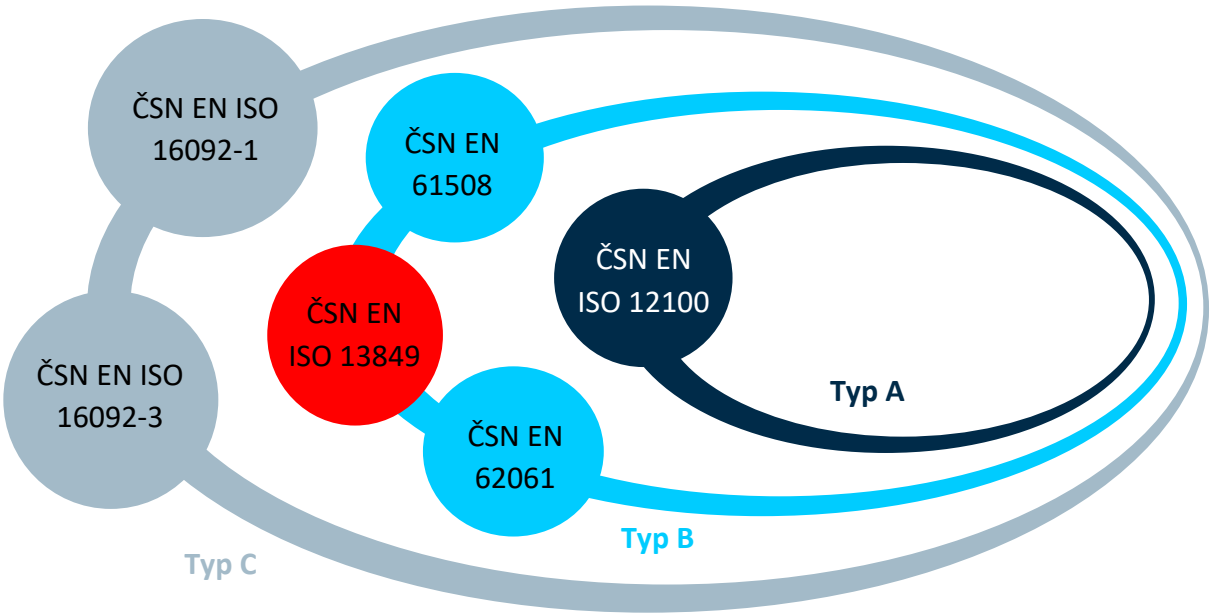
Pokud se obsah normy typu C zásadně liší nebo je v nesouladu s obsahem normy typu A nebo B, má typ C obecně přednost. [6]

Vztah mezi směrnicí Evropského parlamentu a Rady 2006/42/ES a harmonizovanými normami je uveden na obr. 1.




Obr. 1) Souvislost mezi směrnicí pro strojní zařízení a harmonizovanými normami [7]

Vzhledem k cílům a obsahu práce jsou nejrelevantnější normy a jejich hierarchie znázorněny na obr. 2. Z hlediska funkční bezpečnosti bude v praktické části využívána norma ČSN EN ISO 13849, a proto bude dále popsána důkladněji oproti ostatním normám.




Obr. 2) Relevantní normy [7]

# 3 ČSN EN ISO 12100

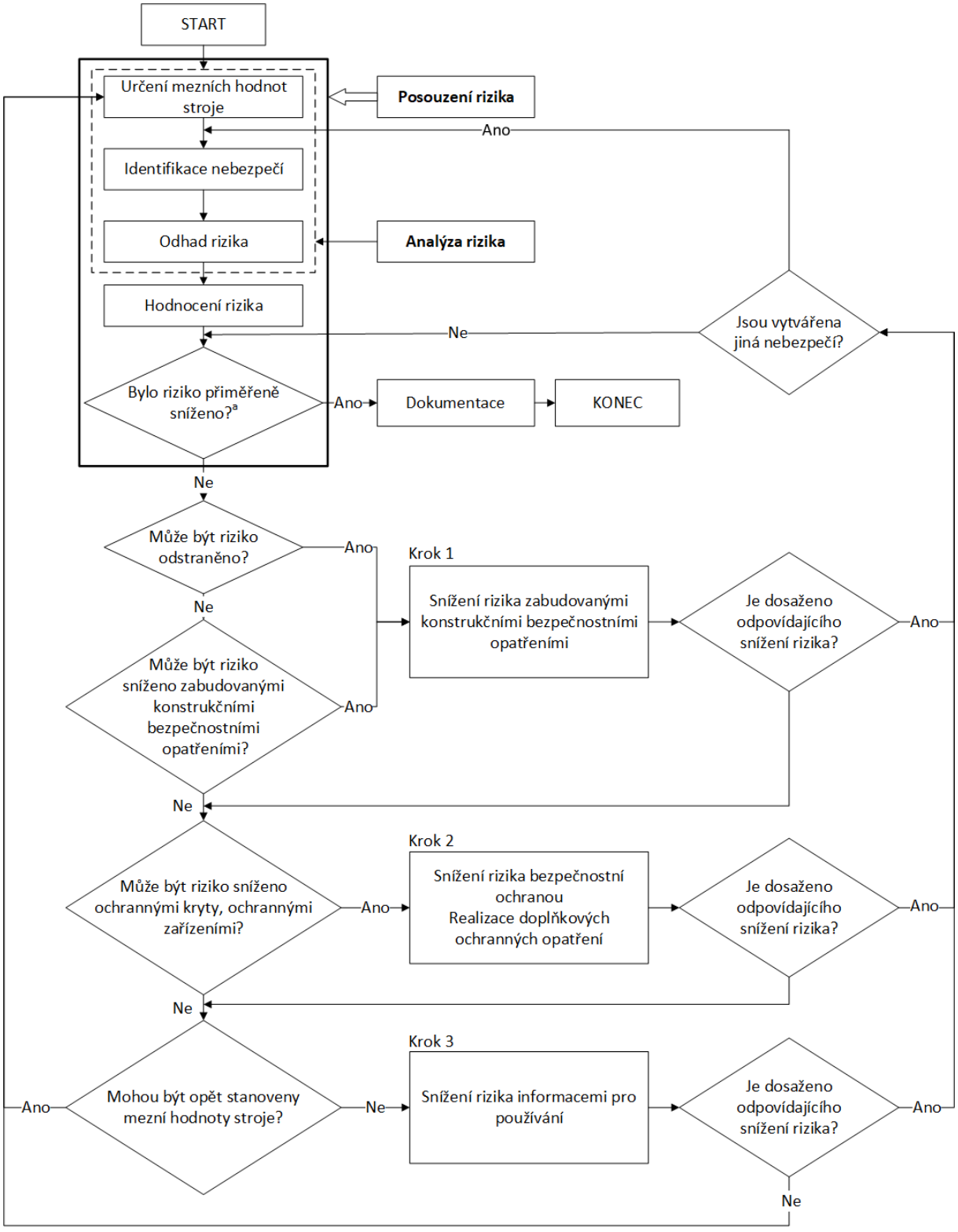
Norma ČSN EN ISO 12100 specifikuje základní pojmy, obecné zásady a postup pro konstrukci bezpečného strojního zařízení.

Nejdůležitější částí zajištění bezpečnosti strojního zařízení je posouzení rizik spojených s daným zařízením v průběhu celého životního cyklu. Povinnost provedení posouzení rizik vyplývá ze směrnice Evropského parlamentu a Rady 2006/42/ES a zodpovídá za něj výrobce, příp. zplnomocněný zástupce.

V rámci posouzení rizik jsou rizika nejprve analyzována. Prvním krokem analýzy je stanovení mezních hodnot strojního zařízení ve všech etapách životního cyklu, kdy je definováno předpokládané použití stroje (provozní režimy, obsluha, potřebné znalosti a dovednosti atd.), dále je vymezen prostor a doba (životnost, údržba) a příp. jsou vymezeny i jiné faktory jako je prostředí, udržovatelnost atd. V této fázi je nutné uvažovat také možnost nesprávného používání strojního zařízení. Poté následuje identifikace nebezpečí opět s přihlédnutím ke všem etapám životního cyklu, přičemž se uvažuje vzájemné působení člověka a stroje, možné stavy stroje a nepředpokládané chování obsluhy nebo předvídatelné selhání stroje. Příklady nebezpečí uvádí norma ČSN EN ISO 12100 v příloze B. Analýza rizik je následně uzavřena odhadem rizika. Odhad vychází ze dvou kritérií – závažnosti úrazu a pravděpodobnosti výskytu tohoto úrazu, které odrážejí i samotnou definici rizika: „*Riziko je kombinace pravděpodobnosti výskytu úrazu a závažnosti tohoto úrazu*.“ [6]

Po analýze rizik následuje zhodnocení rizika za účelem určení, zda je nutné dané riziko snížit či nikoliv. Pro snížení rizik je využívána metoda tří kroků v následujícím pořadí. Prvním a nejefektivnějším krokem je navrhnout a zkonstruovat zařízení tak, aby byla identifikovaná nebezpečí co nejvíce omezena, ideálně úplně odstraněna, např. eliminace ostrých částí či omezení rychlosti pohyblivých prvků. Vzhledem k tomu, že mnohdy není možné pomocí tohoto kroku nebezpečí snížit na požadovanou úroveň, je nutné využít druhý krok, a to bezpečnostní ochranu a doplňková ochranná opatření, např. kryty, optické závory, dvouruční ovládání, kontrolu rychlosti pohybů atd. Pokud není ani druhý krok dostatečný, posledním způsobem zajištění bezpečnosti je informování uživatele o zbytkových rizicích, např. v návodu nebo formou výstražných štítků. Proces posouzení a snížení rizik je schematicky znázorněn na obr. 3. [6]

Posouzení rizik je nutné vnímat nejenom jako povinnost danou Evropskou unií, ale také jako ochranu výrobce v případě škody způsobené výrobkem, kdy je možné využít zdokumentované posouzení rizik jako důkaz, že byla v dostatečné míře přijata opatření pro identifikovaná nebezpečí. [7]




[a] Poprvé je položena otázka, jaký je výsledek počátečního posouzení rizika.

Obr. 3) Znázornění procesu posouzení a snížení rizika

# 4 FUNKČNÍ BEZPEČNOST

Jedním ze způsobů, jak dosáhnout snížení rizik na požadovanou úroveň, je využití ochranných zařízení, jež vykonávají bezpečnostní funkci a jsou závislé na ovládacím (řídícím) systému stroje. S tím je spojeno zajištění dostatečné úrovně funkční bezpečnosti.

Funkční bezpečnost je část celkové bezpečnosti, která se zabývá ochranou před nebezpečími, jež mohou vzniknout v důsledku nekorektní funkce systému. Týká se tedy obzvlášť systémů zajišťujících bezpečnostní funkce, jejichž selhání může vést k poškození zdraví, životního prostředí nebo majetku. Tyto systémy využívají různé technické principy, např. mechanické, hydraulické, pneumatické či elektrické. Funkční bezpečnost řeší nejenom způsob, jak docílit správné funkce těchto systémů, ale i způsob, jak dosáhnout toho, aby bylo zařízení v případě poruchy uvedeno do bezpečného stavu, a nemohlo tak dojít ke škodám. [8]

Základním dokumentem, který pojednává o funkční bezpečnosti, je soubor norem ČSN EN 61508. Z tohoto souboru pak vychází další specifičtější normy týkající se této problematiky, např. ČSN EN ISO 13849 nebo ČSN EN 62061.

Z výše uvedených norem, jimž bude věnována pozornost v následujících podkapitolách, jsou ČSN EN ISO 13849 a ČSN EN 62061 z hlediska směrnice Evropského parlamentu a Rady 2006/42/ES normy harmonizované.

## 4.1 ČSN EN 61508

Tato norma se zabývá systémy, jejichž součástí jsou elektrické, elektronické nebo programovatelné elektronické součásti (příp. kombinace těchto systémů), které jsou určeny k zajištění bezpečnostních funkcí. Může však sloužit i jako základní rámec pro systémy založené na jiných principech. [9]

Aktuální verze souboru z roku 2011 se skládá ze sedmi částí:

- Část 1: Všeobecné požadavky
- Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností
- Část 3: Požadavky na software
- Část 4: Definice a zkratky
- Část 5: Příklady metod určování úrovní integrity bezpečnosti
- Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3
- Část 7: Přehled technik a opatření

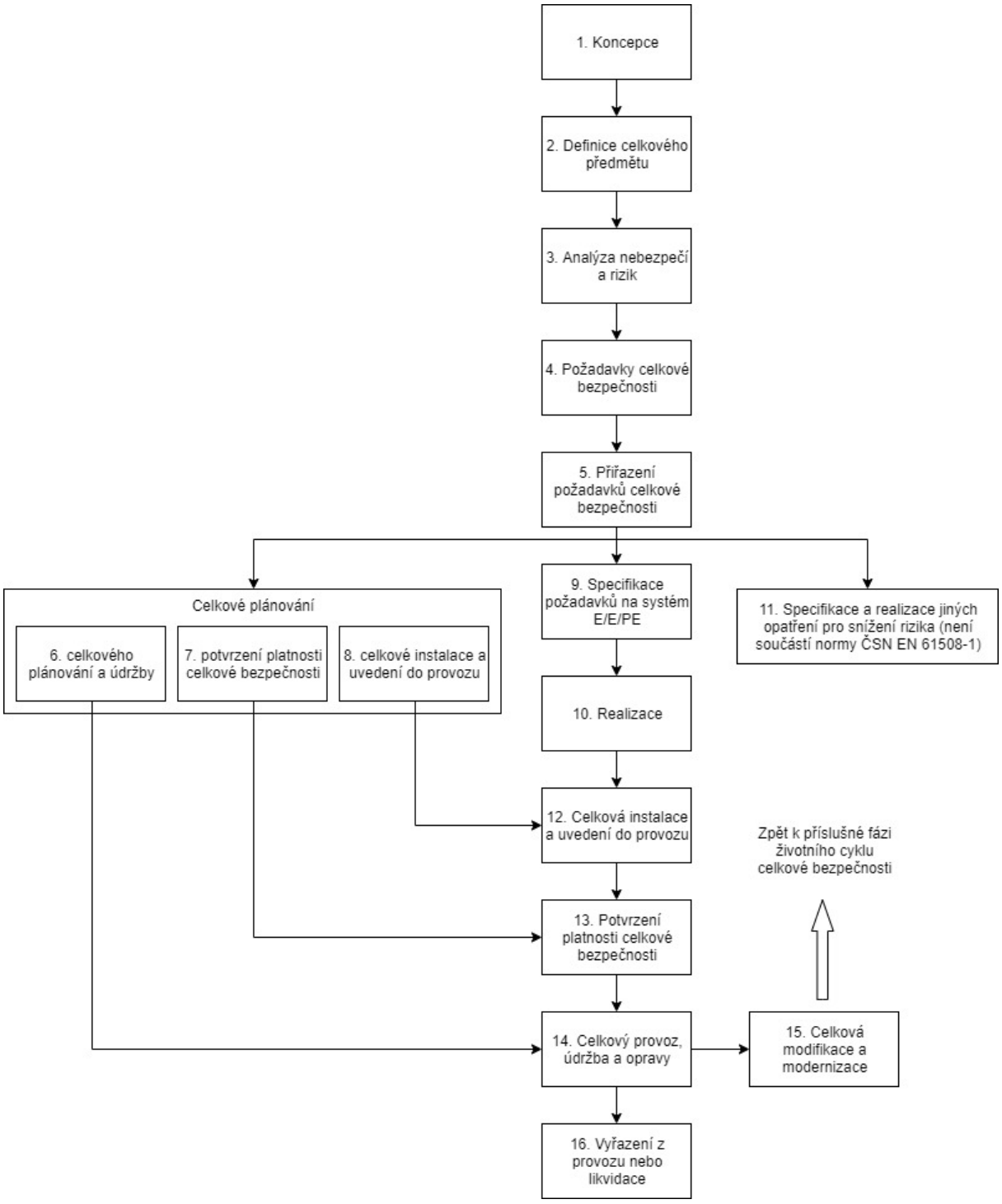
Všeobecné požadavky definované v první části souboru je možné aplikovat ve všech ostatních částech souboru. [9]

Soubor norem ČSN EN 61508 je založen na dvou základních koncepcích, a to na životním cyklu celkové bezpečnosti a na úrovni integrity bezpečnosti (SIL).

*Životní cyklus celkové bezpečnosti*

Životní cyklus celkové bezpečnosti představuje rámec pro systematický postup zajištění požadované funkční bezpečnosti systému a je znázorněn na obr. 4. Pro každou fázi cyklu stanovuje ČSN EN 61508-1 požadavky a cíle. [9]

Podstatou je předpoklad, že funkční bezpečnost je nezávislá na spolehlivosti, tzn. „spolehlivý" nutně neznamená „funkčně bezpečný". Bezpečnost je tak posuzována bez ohledu na schopnost plnit funkci, což umožňuje reálnější pohled na bezpečnost při normálním provozu i v případě poruchy. [11]




Obr. 4) Životní cyklus celkové bezpečnosti [9]

*Úroveň integrity bezpečnosti (SIL)*

Integrita bezpečnosti je definována jako *„pravděpodobnost systému E/E/PE souvisejícího s bezpečností uspokojivě plnit požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu*“. Dle hodnot pravděpodobnosti výskytu nebezpečné poruchy bezpečnostního systému může integrita bezpečnosti nabývat čtyř úrovní, přičemž úroveň 1 je nejnižší a úroveň 4 nejvyšší. Pravděpodobnosti poruchy jsou rozděleny do dvou tabulek (tab. 1 a tab. 2) v závislosti na režimu provozu, který může být s nízkým (malým) vyžádáním, kdy je bezpečnostní funkce v provozu pouze na vyžádání a četnost vyžádání není větší než jedenkrát za rok, nebo s vysokým (velkým) vyžádáním, kdy je bezpečnostní funkce v provozu opět pouze na vyžádání, ale četnost vyžádání je větší než jedenkrát ročně, anebo souvislý, kdy bezpečnostní funkce udržuje zařízení v bezpečném stavu v rámci normálního provozu. [10]

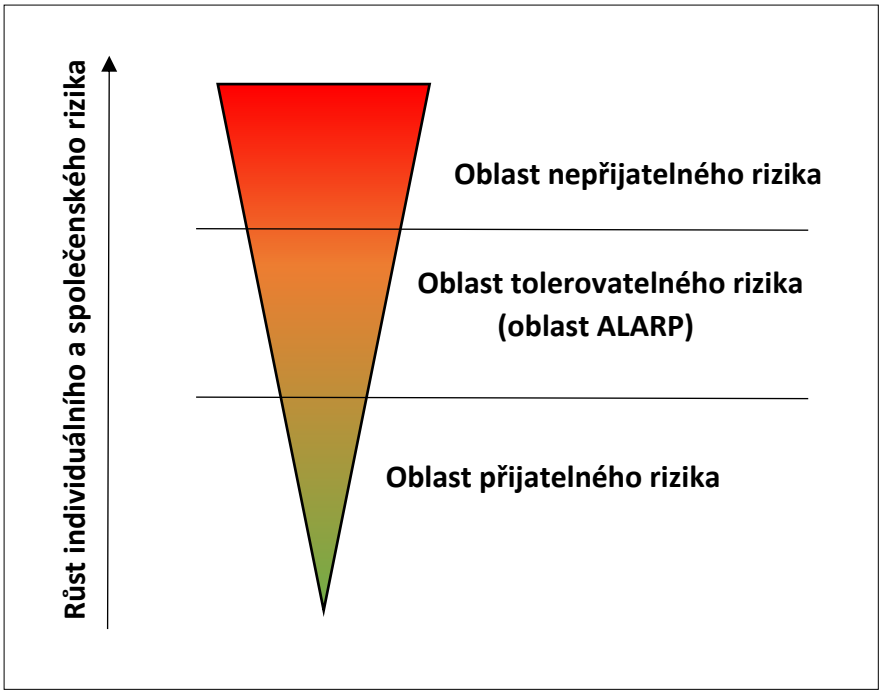
Tab 1) Míry poruch pro bezpečnostní funkci pracující v režimu provozu s nízkým vyžádáním [9]

| **SIL** | **Střední pravděpodobnost nebezpečné poruchy plnit svou bezpečnostní funkci na vyžádání ($PFD_{avg}$)** |
|---|---|
| 1 | $\geq 10^{-5}$ až $< 10^{-4}$ |
| 2 | $\geq 10^{-4}$ až $< 10^{-3}$ |
| 3 | $\geq 10^{-3}$ až $< 10^{-2}$ |
| 4 | $\geq 10^{-2}$ až $< 10^{-1}$ |

Tab 2) Cílové míry poruch pro bezpečnostní funkci pracující v režimu provozu s vysokým nebo nepřetržitým vyžádáním [9]

| **SIL** | **Střední frekvence nebezpečné chyby bezpečnostní funkce za hodinu (PFH)** |
|---|---|
| 1 | $\geq 10^{-9}$ až $< 10^{-8}$ |
| 2 | $\geq 10^{-8}$ až $< 10^{-7}$ |
| 3 | $\geq 10^{-7}$ až $< 10^{-6}$ |
| 4 | $\geq 10^{-6}$ až $< 10^{-5}$ |

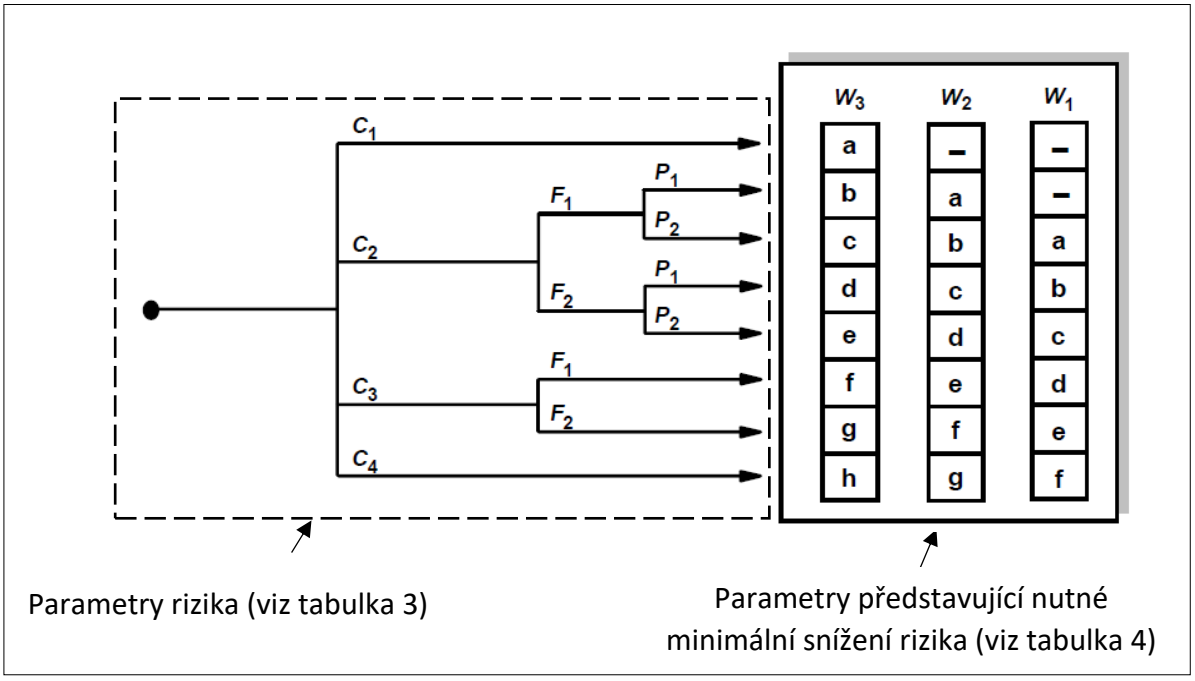
Proto, aby bylo zabráněno iracionálním požadavkům na úroveň integrity bezpečnosti, prosazuje norma ČSN EN 61508-5 princip ALARP (As Low As Reasonable Practicable), který spočívá ve snížení rizik na rozumně proveditelnou úroveň. Riziko je zařazeno do jedné ze tří oblastí (úrovní), které jsou znázorněny na obr. 3. Oblast nepřijatelného rizika představuje část, kdy je riziko natolik vysoké, že nesmí být přijato a musí dojít k jeho snížení alespoň do oblasti tolerovatelného rizika. V této oblasti musí být rozhodnuto, zda je riziko přijatelné či nikoliv s ohledem na náklady spojené s jeho snížením, proveditelnost opatření či jiné aspekty. Poslední oblastí je přijatelná oblast, kde je riziko bezvýznamné. Je však nutné jeho sledování, aby bylo zajištěno, že zůstane na této úrovni. [12]




Obr. 5) ALARP model [12]

Pro samotné stanovení úrovně SIL může být použito několik metod, jejichž obecné zásady jsou popsány rovněž v normě ČSN EN 61508-5. Patří mezi ně např. graf rizik či metoda LOPA.

Graf rizik je založen na určení čtyř parametrů rizika: důsledek nebezpečné události (C), četnost výskytu a doba expozice nebezpečné události (F), možnost vyvarování se nebezpečné události (P) a pravděpodobnost výskytu nebezpečné události (W). Každý z parametrů má přiřazen určitý rozsah hodnot, kterých může nabývat, a to včetně jejich popisu. Příklad takového grafu je uveden na obr. 4, jež je doplněn tabulkami 3 a 4. [12]




Obr. 6) Graf rizik [12]

Tab 3) Parametry rizika [12]

| Parametr rizika | | Popis (klasifikace) |
|---|---|---|
| Důsledek (C) | C1 | Drobné zranění |
| | C2 | Vážné zranění nebo zranění s trvalými následky jedné nebo více osob |
| | C3 | Smrt několika lidí |
| | C4 | Smrt mnoha lidí |
| Četnost výskytu a doba expozice (F) | F1 | Výjimečně |
| | F2 | Často až trvale |
| Možnost vyvarování se nebezpečné události (P) | P1 | Možné za určitých podmínek |
| | P2 | Téměř nemožné |
| Pravděpodobnost výskytu (W) | W1 | Velmi malá pravděpodobnost |
| | W2 | Malá pravděpodobnost |
| | W3 | Relativně vysoká pravděpodobnost |

Tab 4) Parametry představující nutné minimální snížení rizika [12]

| Nezbytné minimální snížení rizika | SIL |
|---|---|
| - | Žádné bezpečnostní požadavky |
| a | Žádné speciální bezpečnostní požadavky |
| b, c | 1 |
| d | 2 |
| e, f | 3 |
| g | 4 |
| h | Bezpečnostní systém je nedostatečný |

Metoda LOPA (Layer Of Protection Analysis = analýza vrstev ochrany) slouží k identifikaci nebezpečí, bezpečnostních funkcí a požadavků na SIL. U každého nebezpečí jsou popsány důsledky a příčiny jeho vzniku, závažnost a pravděpodobnost iniciace. Dále jsou určeny ochranné vrstvy, které sníží pravděpodobnost iniciace nebezpečné události nebo zmírní její dopad (např. kontrolní systémy či hlásiče), a jejich $PFD_{avg}$. Pro každou příčinu je poté vypočítána „frekvence průběžné události“ a součtem těchto frekvencí lze získat celkovou frekvenci, která je následně porovnána s tolerovatelnou úrovní. Pokud celková frekvence překročí tolerovatelnou úroveň, musí být zváženo řešení ve formě bezpečnostního systému. V tomto případě lze SIL zjistit podílem tolerovatelné úrovně a celkové frekvence, čímž je získána celková hodnota $PFD_{avg}$ a jejím porovnáním s hodnotami uvedené v tabulce 1 této práce je stanoveno požadované SIL. [12]

## 4.2 ČSN EN ISO 13849

ČSN EN ISO 13849 je norma, která se týká bezpečnostních částí ovládacích systémů (SRP/CS) využívajících různé druhy technologií a energií (např. elektrické, hydraulické, pneumatické aj.).

Skládá se ze dvou částí:

- Část 1: Obecné zásady pro konstrukci (z roku 2017)
- Část 2: Ověřování platnosti (z roku 2013)

První část uvádí základní pojmy, požadavky a postup pro návrh bezpečnostních částí ovládacího systému. Druhá část je věnována postupům a podmínkám pro ověřování platnosti SRP/CS. Konkrétně jsou pomocí analýz a zkoušení validovány specifikované bezpečnostní funkce, dosažené kategorie a úrovně vlastností. [13,14]

*Identifikace a popis bezpečnostních funkcí*

Prvním krokem je identifikace bezpečnostních funkcí, jež budou realizovány pomocí SRP/CS. To by mělo být provedeno na základě posouzení rizik. U každé bezpečnostní funkce musí být popsáno, jakým způsobem je spuštěna, bezpečný stav a způsob, jakým ho bude dosaženo (reakce na nebezpečnou situaci). Kromě toho musí být také dodrženy požadavky týkající se vlastností dané bezpečnostní funkce uvedené přímo v ČSN EN ISO 13849 a v příslušných normách týkajících se jednotlivých bezpečnostních funkcí, parametrů nebo vlastností. [13]

*Určení požadované úrovně vlastností (PLr)*

Pro každou bezpečnostní funkci musí být určena požadovaná úroveň vlastností $PL_r$. Norma popisuje celkem pět úrovní vlastností – a až f, přičemž úroveň a je nejnižší a úroveň f nejvyšší. Úrovně jsou definovány pomocí průměrné pravděpodobnosti nebezpečné poruchy za hodinu $PFH_D$ a jsou uvedeny v tabulce 5. [13]

Tab 5) Úrovně vlastností (PL) [13]

| **PL** | **Průměrná pravděpodobnost nebezpečné poruchy za hodinu ($PFH_D$) [1/h]** |
|---|---|
| a | $\geq 10^{-5}$ až $< 10^{-4}$ |
| b | $\geq 3{\cdot}10^{-6}$ až $< 10^{-5}$ |
| c | $\geq 10^{-6}$ až $< 3{\cdot}10^{-6}$ |
| d | $\geq 10^{-7}$ až $< 10^{-6}$ |
| e | $\geq 10^{-8}$ až $< 10^{-7}$ |

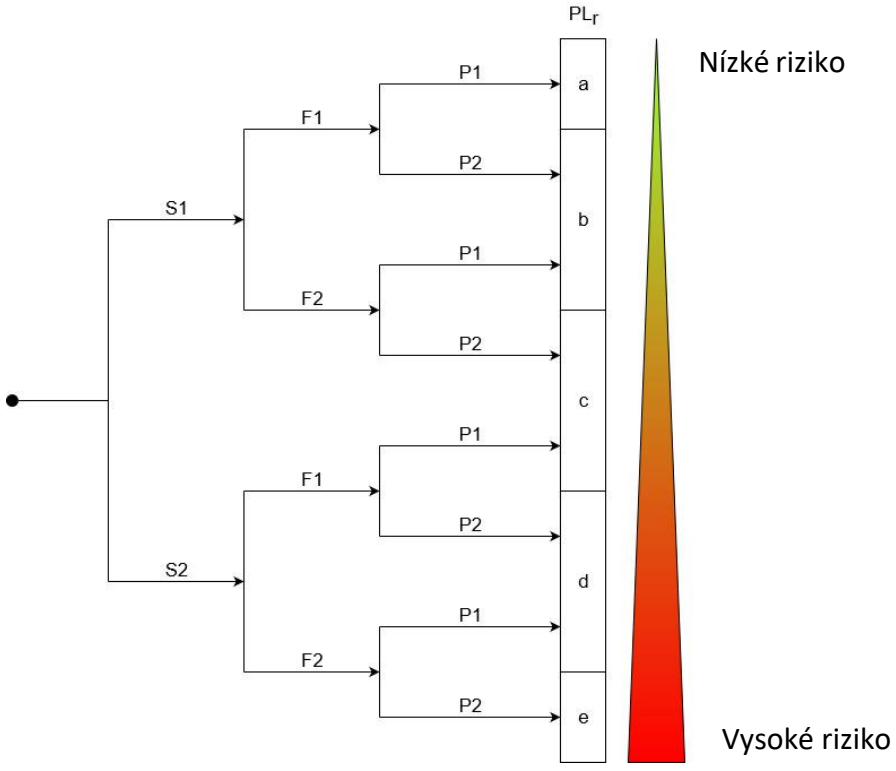
Pro určení požadované úrovně vlastností $PL_r$, která je poté porovnávána s úrovní vlastností daného SRP/CS, může být použita metoda velice podobná grafu rizik, jež byl popsán v kapitole 4.1. Jedná se o metodu, jejíž využití není povinné a předpokládá 100% pravděpodobnost výskytu nebezpečné události. [13]

Každý z parametrů S (závažnost zranění), F (četnost a/nebo doba vystavení nebezpečí) a P (možnost vyloučení nebezpečné události) může nabývat hodnot 1 nebo 2. Popis, pomocí nějž lze rozhodnout o hodnotách jednotlivých parametrů, je uveden v tabulce 5. [13]

Tab 6) Parametry pro určení $PL_r$ [13]

| Parametr | | Popis |
|---|---|---|
| Závažnost (S) | 1 | Lehké zranění (pohmoždění, tržné rány bez komplikací atd.) |
| | 2 | Závažné zranění (smrt nebo zranění s trvalými následky, např. amputace) |
| Četnost a/nebo doba vystavení nebezpečí (F) | 1 | Celková doba vystavení nepřesáhne 1/20 celkové provozní doby, četnost není vyšší než jednou za 15 min |
| | 2 | Osoba je vystavena nebezpečí často nebo trvale, četnost je vyšší než jednou za 15 min |
| Možnost vyloučení nebezpečné události (P) | 1 | Reálná šance k zabránění nebezpečí nebo je možné snížení jeho vlivu |
| | 2 | Šance pro odvrácení nebezpečí je malá nebo žádná a jeho vliv není možné snížit |

Na základě hodnot parametrů je poté z grafu (obr. 7) určena požadovaná úroveň vlastností $PL_r$.

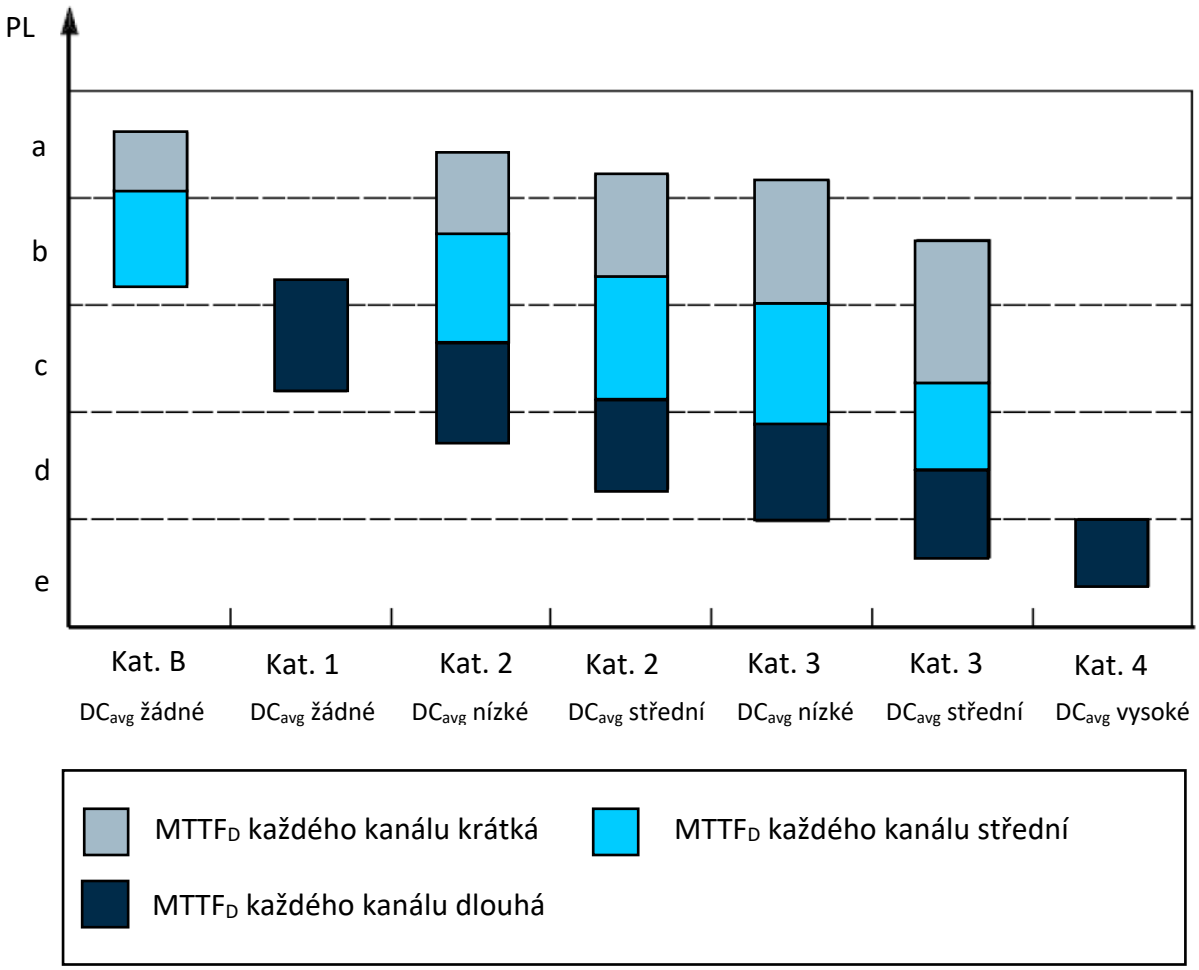



Obr. 7) Graf pro určení $PL_r$ [13]

Kromě použití této metody lze zjistit požadavky na $PL_r$ také v normách typu C. Příkladem takové normy je ČSN EN ISO 16092-3, která definuje minimální $PL_r$ pro bezpečnostní funkce a také kategorie pro jednotlivé části jako jsou vstupní zařízení, logika a výstupní zařízení.

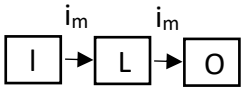
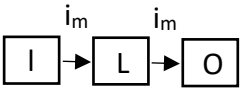
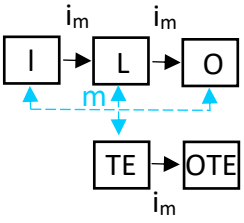
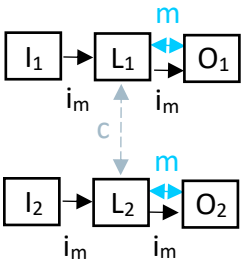
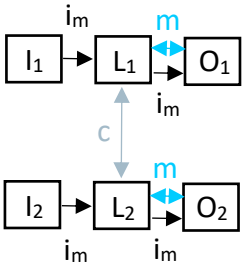
*Návrh SRP/CS*

V rámci návrhu SRP/CS by měla být nejprve zvolena kategorie. ČSN EN ISO 13849-1 popisuje pět kategorií (B, 1, 2, 3 a 4), jež „*klasifikují SRP/CS vzhledem k odolnosti proti závadám a jejich následnému chování v podmínce závady, kterého je dosaženo konstrukčním uspořádáním částí, detekcí závady a/nebo jejich spolehlivostí*“. Volbu vhodné kategorie pro dosažení specifického $PL_r$ může usnadnit obrázek č. 8 a tabulka č. 7, kde jsou jednotlivé kategorie stručně popsány, přičemž upřesnění úrovní střední doby do poruchy ($MTTF_D$) je uvedeno v tabulce 8 a diagnostického pokrytí (DC) v tabulce 9. [13]




Obr. 8) Vztah mezi kategoriemi, $DC_{avg}$, $MTTF_D$ každého kanálu a PL [13]

Tab 7) Stručný popis jednotlivých kategorií [13]

| | Požadavky | Architektura | $MTTF_D$ každého kanálu | $DC_{avg}$ | Opatření proti CCF | Max. PL |
|---|---|---|---|---|---|---|
| **B** | Odolnost SRP/CS a/nebo ochranných zařízení a jejich komponent vůči očekávaným vlivům a použití základních bezpečnostních zásad |  | Krátká až střední | Žádné | ne | b |
| **1** | Splnění požadavků kategorie B, použití osvědčených komponent a osvědčených bezpečnostních zásad |  | Dlouhá | Žádné | ne | c |
| **2** | Splnění požadavků kategorie B, použití osvědčených bezpečnostních zásad a kontrola bezpečnostní funkce v daných intervalech ovládacím systémem stroje |  | Krátká až dlouhá | Nízké až střední | ano | d |
| **3** | Splnění požadavků kategorie B, použití osvědčených bezpečnostních zásad a navržení bezpečnostních částí tak, aby jejich závady nevedly ke ztrátě bezpečnostní funkce a každá závada byla detekována, kdykoliv je to rozumně možné |  | Krátká až dlouhá | Nízké až střední | ano | e |
| **4** | Splnění požadavků kategorie B, použití osvědčených bezpečnostních zásad a navržení bezpečnostních částí tak, aby jejich závady nevedly ke ztrátě bezpečnostní funkce a každá závada byla detekována při nebo před nejbližší bezpečnostní funkcí, přičemž v případě, kdy to není možné, nesmí vést nahromadění nedetekovatelných závad ke ztrátě bezpečnostní funkce |  | Dlouhá | Vysoké | ano | e |

Pozn.: u architektury pro kategorii 4 je diagnostické pokrytí vyšší než u kategorie 3.

Legenda k symbolům použitým v tabulce 7:

$i_m$ ..... prostředky vzájemného propojení
c ..... křížové monitorování
m ..... monitorování
I, $I_1$, I2 ..... vstupní zařízení
L, $L_1$, $L_2$ ..... logika
O, $O_1$, $O_2$ ..... výstupní zařízení

Tab 8) Označení $MTTF_D$ [13]

| **Označení doby každého kanálu** | **Rozsah doby každého kanálu** |
|---|---|
| Krátká | 3 roky ≤ $MTTF_D$ < 10 roků |
| Střední | 10 roků ≤ $MTTF_D$ < 30 roků |
| Dlouhá | 30 roků ≤ $MTTF_D$ ≤ 100 roků |

Tab 9) Označení DC [13]

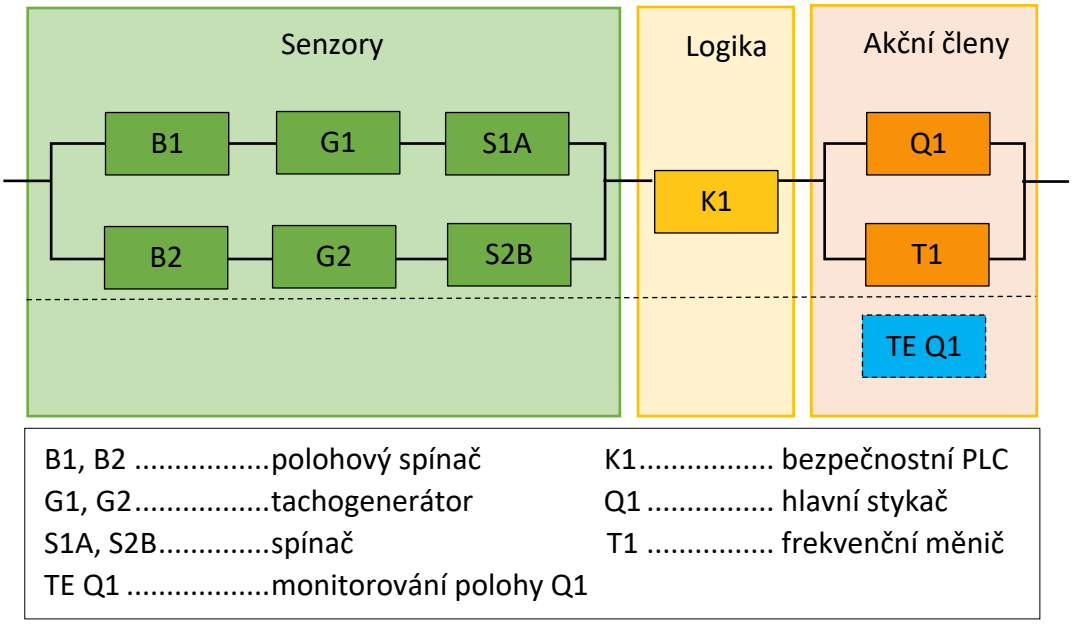
| **Označení** | **Rozsah** |
|---|---|
| Žádné | DC < 60 % |
| Nízké | 60 % ≤ DC < 90 % |
| Střední | 90 % ≤ DC < 99 % |
| Vysoké | 99 % ≤ DC |

Dále je nutné identifikovat SRP/CS (může být jedna nebo více), které se budou podílet na bezpečnostní funkci. Bezpečnostní funkce je obvykle tvořena kombinací:

- vstupních prvků, které detekují nebezpečnou situaci,
- prvků logiky, jež vyhodnocují informace získané ze vstupních prvků a stavu zařízení,
- výstupních prvků ovládajících pohony zařízení.

Součástí bezpečnostní funkce mohou být také zkušební zařízení (diagnostické prvky), které kontrolují správnou funkci daného prvku.

Následně je sestaveno bezpečnostní blokové schéma, jež znázorňuje logickou strukturu bezpečnostní funkce. Jednotlivé části mohou být spojeny sériově (porucha jednoho bloku způsobí poruchu celého kanálu, čímž může dojít ke ztrátě bezpečnostní funkce) nebo paralelně (bezpečnostní funkce nebude vykonána pouze v případě, kdy u všech kanálů dojde k poruše). Pokud jsou využita zkušební zařízení, která neovlivní bezpečnostní funkci v případě jejich poruchy, mohou být znázorněna odděleně od jednotlivých bloků. Příklad blokového digramu je uveden na obr. 9. [13]




Obr. 9) Příklad blokového diagramu [7]

*Odhad úrovně vlastností (PL)*

Dalším krokem je odhad PL. Pro každé SRP/CS musí být odhadnuta hodnota PL s ohledem na [13]:

- střední doby do nebezpečné poruchy ($MTTF_D$) pro jednotlivé komponenty,
- diagnostické pokrytí (DC),
- poruchy se společnou příčinou (CCF),
- strukturu,
- chování bezpečnostní funkce v podmínce/podmínkách,
- bezpečnostní software,
- systematické poruchy,
- schopnost vykonávat bezpečnostní funkci v očekávaných podmínkách prostředí.

Výše uvedené body lze rozdělit na kvantitativní hlediska ($MTTF_D$, DC, CCF, struktura) a nezjištěná kvalitativní hlediska, jež se podílí na chování SRP/CS (chování bezpečnostní funkce v podmínce/podmínkách, bezpečnostní software, systematické poruchy a podmínky prostředí). [13]

Pro kvantitativní hlediska je možné využít zjednodušenou metodu spočívající v odhadu PL na základě hodnot $MTTF_D$ a DC a kategorii (tab. 10)

Tab 10) Zjednodušený postup pro určení PL

| **Kategorie** | **B** | **1** | **2** | **2** | **3** | **3** | **4** |
|---|---|---|---|---|---|---|---|
| **$DC_{avg}$** | žádné | žádné | nízké | střední | nízké | střední | vysoké |
| **$MTTF_D$ každého kanálu** | | | | | | | |
| Krátká | a | - | a | b | b | c | - |
| Střední | b | - | b | c | c | d | - |
| Dlouhá | - | c | c | d | d | d | e |

$MTTF_D$ musí být určena pro každý kanál a její hodnotu pro jednotlivé komponenty lze získat třemi způsoby [13]:

a) použitím údajů od výrobce;
b) použitím hodnot z příloh C a D normy ČSN EN 13849-1 nebo výpočtem pro komponenty z hodnoty $B_{10D}$ dle rovnice 1:

$$\mathrm{MTTF_D} = \frac{B_{10D}}{0{,}1 \cdot n_{op}} \tag{1}$$

kde $B_{10D}$ je počet cyklů do 10 % nebezpečných selhání komponentů (pro pneumatické a elektromechanické komponenty) a $n_{op}$ je střední počet ročního provozu, který lze vypočítat pomocí rovnice 2 z $d_{op}$ (střední doba provozu v hodinách za den), $h_{op}$ (střední doby provozu ve dnech za rok) a $t_{cyklu}$ (střední doba mezi začátky dvou po sobě následujících cyklů komponenty v sekundách/cyklus).

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600}{t_{cyklu}} \tag{2}$$

V případě, že výrobce uvádí pouze hodnotu $B_{10}$ (střední počet cyklů do výpadku 10 % komponent), je možné $B_{10D}$ vypočítat dle rovnice 3 jako:

$$B_{10D} = 2B_{10} \tag{3}$$

Pro každý kanál poté platí rovnice č. 4:

$$\frac{1}{\mathrm{MTTF_D}} = \sum_{i=1}^{n} \frac{1}{\mathrm{MTTF_{D}}i} \tag{4}$$

Pokud $MTTF_D$ kanálů nejsou stejné, musí být buď použita nižší z hodnot, nebo může být hodnota vypočítána pomocí rovnice 5.

$$\mathrm{MTTF_D} = \frac{2}{3}\left[\mathrm{MTTF_{DC1}} + \mathrm{MTTF_{DC2}} - \frac{1}{\frac{1}{\mathrm{MTTF_{DC1}}} + \frac{1}{\mathrm{MTTF_{DC2}}}}\right] \tag{5}$$

c) použitím hodnoty 10 let.

Na základě získané hodnoty lze potom zařadit $MTTF_D$ do jedné ze tří kategorií, které jsou uvedeny v tab. 8.

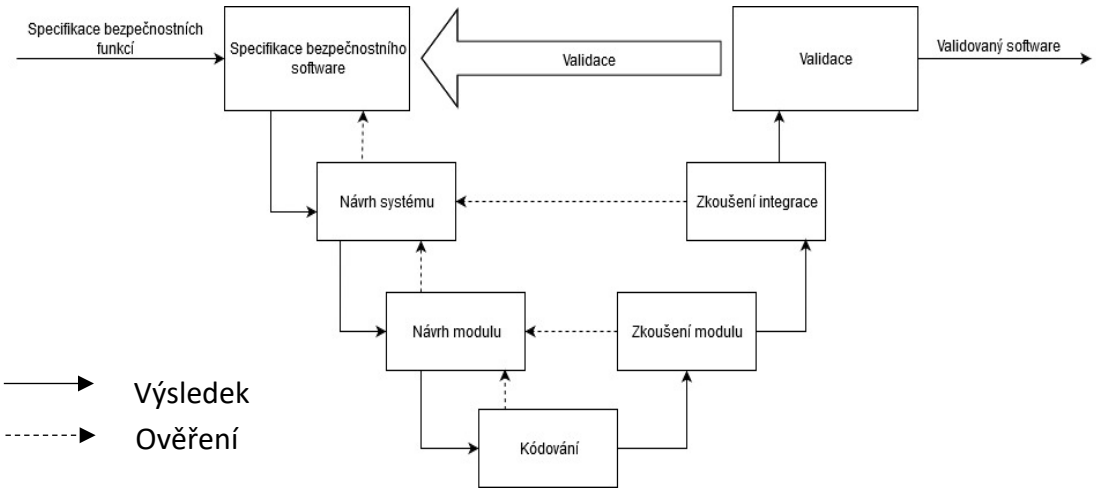
Diagnostické pokrytí vyjadřuje míru účinnosti diagnostiky. Pro jeho odhad uvádí norma ČSN EN ISO 13849-1 zjednodušený postup, který je založen na použití hodnot z tabulky v příloze E pro všechny komponenty s detekcí poruch. K detekci poruch u jednotlivých komponent může být použito např. přímé nebo nepřímé monitorování. Následně je průměrné diagnostické pokrytí vypočteno dle rovnice 6, přičemž výsledná hodnota $DC_{avg}$ je vyjádřena pomocí jedné z úrovní uvedených v tab. 7. [13]

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \cdots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \cdots + \frac{1}{MTTF_{DN}}} \tag{6}$$

Poruchy se společnou příčinou jsou dle ČSN EN ISO 13849-1 definovány jako „*poruchy různých objektů způsobené jednou událostí, přičemž tyto poruchy nejsou následky jedna druhé*“. Patří mezi ně např. výpadek energie. SRP/CS kategorií 2, 3 a 4 musejí být dostatečně opatřena proti těmto poruchám. V příloze F normy je uveden seznam nejdůležitějších opatření a jejich bodové hodnocení, které představuje účinnost každého opatření. Např. použitím osvědčených komponent lze získat 5 bodů, fyzickým oddělením jednotlivých drah signálu lze získat 20 bodů a aplikací obou opatření 25 bodů. Lze však přiřazovat pouze plný počet bodů nebo žádné body, a to i v případě, že je opatření splněno částečně. Celkově je možné získat použitím různých opatření až 100 bodů, přičemž pro splnění požadavku je nutné dosáhnout celkového počtu alespoň 65 bodů. [13]

Kvalitativních hledisek může být dosaženo realizací opatření proti systematickým poruchám a opatření týkajících se vývoje softwaru. Systematické poruchy jsou poruchy “*související rozhodujícím způsobem s určitou příčinou, která může být vyloučena pouze modifikací návrhu nebo výrobního procesu, provozních postupů, dokumentací nebo jiných relevantních faktorů*”. Opatření jsou uvedena v příloze G normy ČSN EN ISO 13849-1 a zahrnují opatření nejenom pro vyloučení systematických chyb, ale i pro jejich řízení. [13]

Norma definuje také požadavky na bezpečnostní software. Cílem je vyloučení závad, které mohou být způsobeny činnostmi v rámci celého životního cyklu softwaru a dosáhnout jeho čitelnosti, srozumitelnosti, kontrolovatelnosti a udržovatelnosti. Při vývoji je používán V-model platný pro vestavěný i aplikační software (obr. 10). [13]




Obr. 10) Zjednodušený V-model [13]

*Porovnání PL a PLr*

Hodnota PL musí být stejná nebo vyšší než $PL_r$. V případě, že tomu tak není, je nutné navrhnout bezpečnostní funkci jinak a znovu odhadnout PL na základě nového návrhu. Proces musí být opakován, dokud nebude splněno $PL \geq PL_r$. [13]

*Validace (ověření platnosti)*

Validace slouží k ověření, že byly splněny všechny relevantní požadavky normy ČSN EN ISO 13849-1, a jak již bylo zmíněno, je jí věnována ČSN EN ISO 13849-2. Platnost může být ověřena analýzou a případně i zkoušením, pokud není analýza dostatečná. Pro ověření analýzou mohou být využity dvě techniky: „shora dolů“ (deduktivní, např. FTA, ETA) nebo „zdola nahoru“ (induktivní, např. FMEA, FMECA). Zkoušení je realizováno ručně nebo automaticky. [14]

## 4.3 ČSN EN 62061

Norma ČSN EN 62061 se zabývá návrhem, začleněním a potvrzením platnosti elektrických, elektronických a programovatelných elektronických řídicích systémů, které souvisí s bezpečností (SRECS) u strojů. [15]

Pro návrh všech SRECS musí být vypracován plán funkční bezpečnosti, pomocí nějž budou popsány všechny relevantní činnosti a jejich řízení – od specifikace požadavků na řídicí funkci související s bezpečností (SRCF) až po modifikaci SRECS. [15]

*Specifikace SRCF*

U každé bezpečnostní funkce ve formě SRECS musí být s využitím výsledků posouzení rizik a pracovních charakteristik stroje specifikovány funkční požadavky na SRCF (popis, požadované časové odezvy, četnost funkce atd.) a požadavky na integritu bezpečnosti SRCF ve formě SIL. [15]

Norma popisuje celkem tři hladiny (úrovně) integrity bezpečnosti definované pomocí $PFH_D$, které jsou uvedeny v tabulce 11. [15]

Tab 11) Hladiny integrity bezpečnosti [15]

| **Hladina integrity bezpečnosti** | **Pravděpodobnost nebezpečné poruchy za hodinu ($PFH_D$)** |
|---|---|
| 1 | $\geq 10^{-8}$ až $< 10^{-7}$ |
| 2 | $\geq 10^{-7}$ až $< 10^{-6}$ |
| 3 | $\geq 10^{-6}$ až $< 10^{-5}$ |

Pro stanovení SIL jsou využívány čtyři parametry: závažnost škody (Se), četnost a doba trvání ohrožení osob nebezpečím (Fr), pravděpodobnost výskytu nebezpečných událostí (Pr) a možnost vyvarovat se nebo omezit škodu (Av). Hodnoty, kterých mohou nabývat a jejich upřesnění je uvedeno v tabulce 12. [15]

Na základě jednotlivých parametrů lze pak rozhodnout pomocí matice (tab. 13) o hodnotě SIL, přičemž třída (CI) představuje součet hodnot Fr, Pr a Av. Pokud je kombinací získáno (OM), mělo by být použito jiné opatření. [15]

Tab 12) Jednotlivé třídy pro určení SIL [15]

| **Parametr** | | **Popis** |
|---|---|---|
| Závažnost škody (Se) | 1 | Lehké zranění vyžadující ošetření první pomoci (škrábance, pohmožděniny atd.) |
| | 2 | Zranění s přechodnými následky vyžadující ošetření praktickým lékařem (závažnější tržné rány, bodné rány atd.) |
| | 3 | Těžké zranění s trvalými následky nebo těžká zranění bez trvalých následků; lze pokračovat ve stejné práci (zlomeniny, ztráta prstů atd.) |
| | 4 | Smrtelné zranění nebo zranění s trvalými následky; nelze pokračovat ve stejné práci (ztráta oka nebo paže atd.) |
| Četnost a doba trvání ohrožení osob nebezpečím (Fr)* | 2 | < 1 za rok |
| | 3 | < 1 za 2 týdny až ≥ 1 za rok |
| | 4 | < 1 za den až ≥ 1 za 2 týdny |
| | 5 | < 1 za h až ≥ 1 za den |
| | 5 | ≤ 1 za h |
| Pravděpodobnost výskytu nebezpečných událostí (Pr) | 1 | Zanedbatelná |
| | 2 | Výjimečná |
| | 3 | Možná |
| | 4 | Pravděpodobná |
| | 5 | Velmi vysoká |
| Možnost vyvarovat se nebo omezit škodu (Av) | 1 | Pravděpodobné |
| | 3 | Možné za určitých podmínek |
| | 5 | Nemožné |

* Platí pro dobu trvání > 10 min; v případě, že je doba trvání kratší, může být hodnota zmenšena na nejbližší nižší úroveň (neplatí pro ≤ 1 za h)

Tab 13) Matice určení SIL [15]

| **Závažnost (Se)** | **Třída (CI)** | | | | |
|---|---|---|---|---|---|
| | **4** | **5-7** | **8-10** | **11-13** | **14-15** |
| **4** | SIL 2 | SIL 2 | SIL 2 | SIL 3 | SIL 3 |
| **3** | | (OM) | SIL 1 | SIL 2 | SIL 3 |
| **2** | | | (OM) | SIL 1 | SIL 2 |
| **1** | | | | (OM) | SIL 1 |

Pokud je SIL dáno normou typu C, má obecně tato hodnota přednost před hodnotou získanou výše uvedeným způsobem. [15]

*Návrh a integrace SRECS*

Dalším krokem je samotný návrh a integrace SRECS tak, aby byly splněny požadavky specifikované v prvním kroku a příp. i požadavky týkající se bezpečnosti softwaru. [15]

Obecně každé SRECS musí splňovat požadavky na [15]:

- integritu bezpečnosti hardwaru,
- systematickou integritu bezpečnosti,
- chování SRECS při detekci poruchového stavu,
- návrh a vývoj softwaru souvisejícího s bezpečností.

Kromě toho musí být návrh SRECS přizpůsoben lidským schopnostem a omezením s ohledem na uživatele, a to i včetně předvídatelného chybného použití. [15]

*Informace pro použití SRECS*

Spolu se SRECS musí být dodány uživatelům relevantní informace tak, aby mohly být vypracovány postupy pro správnou instalaci, používání a údržbu stroje, a byla tak zachována požadovaná úroveň funkční bezpečnosti. Dokumentace musí zahrnovat např. úplný popis zařízení, instalace a montáže, schémata zapojení, interval kontrolní zkoušky nebo dobu životnosti atd. [15]

*Validace (potvrzení platnosti)*

Aby mohlo být dokázáno, že SRECS splňuje specifikované požadavky, je nutné provést jeho kontrolu a zkoušení. To zahrnuje např. funkční zkoušky, zkoušky odolnosti proti elektromagnetickému rušení či simulace vad. [15]

*Modifikace*

SRECS může být modifikováno např. na základě zkušeností při nehodách, změn ve specifikaci bezpečnostních požadavků či úprav stroje nebo jeho provozních režimů. Vliv modifikace musí být vždy analyzován, aby byla ověřena její účinnost a působení na funkční bezpečnost. [15]

## 4.4 Porovnání norem ČSN EN ISO 13849 a ČSN EN 62061

Vzhledem k tomu, že ČSN EN ISO 13849 a ČSN EN 62061 jsou normy vytvořené na základě souboru norem ČSN EN 61508 a v některých částech se na něj odkazují, budou v této části porovnány pouze tyto dvě normy. Normy nemohou být kombinovány a musí být předem určeno, podle které normy bude funkční bezpečnost řešena.

Obě normy se zabývají požadavky týkající se návrhu a realizace bezpečnostních částí ovládacích systémů u strojních zařízení a jak již bylo zmíněno v úvodu kapitoly 5, obě jsou zařazeny mezi harmonizované normy pro strojní zařízení. Za účelem usnadnit volbu mezi těmito normami byl vydán dokument ISO/TR 23849, který objasňuje použití obou norem. [16]

Největším rozdílem je aplikace norem z pohledu použitých technologií a energií pro realizaci systémů. Zatímco norma ČSN EN ISO 13849 je aplikovatelná pro všechny druhy systémů, ČSN EN 62061 je určena pouze pro elektrické, elektronické a programovatelné elektronické systémy. [16]

Další podstatný rozdíl spočívá ve způsobu určení úrovně spolehlivosti systému. ČSN EN ISO 13849 využívá pět úrovní PL (a-e), přičemž požadovaná úroveň je získána pomocí grafu. ČSN EN 62061 uvádí matici, na jejíž základě je zjištěno SIL, které může nabývat hodnot 1 až 3. Ačkoliv PL i SIL jsou určeny průměrnou pravděpodobností poruchy za hodinu ($PFH_D$) a existuje mezi nimi převodní vztah uvedený v tabulce 14, není možné tyto normy při návrhu bezpečnostní funkce kombinovat, jak již bylo zmíněno. [16]

Tab 14) Vztah mezi PL a SIL [16]

| **PL** | **Průměrná pravděpodobnost poruchy za hodinu ($PFH_D$)** | **SIL** |
|---|---|---|
| a | $\geq 10^{-5}$ až $< 10^{-4}$ | - |
| b | $\geq 3 \cdot 10^{-6}$ až $< 10^{-5}$ | 1 |
| c | $\geq 10^{-6}$ až $< 3 \cdot 10^{-6}$ | 1 |
| d | $\geq 10^{-7}$ až $< 10^{-6}$ | 2 |
| e | $\geq 10^{-8}$ až $< 10^{-7}$ | 3 |

Obecně, pokud jsou v normě typu C zabývající se bezpečností daného strojního zařízení uvedeny požadované hodnoty v podobě PL, měla by být použita norma ČSN EN ISO 13849. V případě, že jsou uvedeny požadavky ve formě SIL, je vhodné použít ČSN EN 62061.

Vzhledem k tomu, že praktická část je zaměřena na funkční bezpečnost hydraulického lisu, kde budou řešena i neelektrická zařízení, a norma ČSN EN ISO 16092-3, jež se zabývá bezpečností hydraulických lisů (viz další kapitola), udává požadavky týkající se funkční bezpečnosti v podobě PL, bude dále využívána norma ČSN EN ISO 13849.

# 5 ISO 16092

Norma stanovuje požadavky a opatření týkající se bezpečnosti lisů sloužících ke tváření kovů (příp. i jiných materiálů jako plasty atd.) za studena. Jedná se o normu typu C, která je vhodná pro konstruktéry, výrobce a dodavatele. [17]

Skládá se celkem ze čtyř částí. První část se zabývá obecnými požadavky na bezpečnost lisů a spolu s ní musí být použita jedna ze zbývajících částí dle typu lisu. Druhá část je tedy věnována mechanickým lisům, třetí část hydraulickým lisům a čtvrtá část pneumatickým lisům. [17]

Pro tuto práci jsou relevantní části 1 a 3, které jsou harmonizované pro strojní zařízení a byly také jako jediné části této normy přejaty překladem ve formě ČSN EN ISO 16092-1 a ČSN EN ISO 16092-3.

V ČSN EN ISO 16092-1 je uveden seznam významných nebezpečí a situací, jež vyžadují opatření pro snížení nebo odstranění rizik, viz tabulka 15. [17]

Tab 15) Významná nebezpečí [17]

| Druh nebezpečí | Příklady původu nebezpečí |
|---|---|
| Mechanická nebezpečí | Pružné elementy, tíže, pohybující se elementy, rotující elementy atd. |
| Elektrická nebezpečí | Zkrat, živé části, elektromagnetické jevy atd. |
| Tepelná nebezpečí | Předměty nebo materiály s vysokou nebo nízkou teplotou atd. |
| Nebezpečí hluku | Pohybující se části, opotřebení částí, kavitační jevy atd. |
| Nebezpečí vibrací | Nevyvážené rotující části, nesouosost pohybujících se částí atd. |
| Nebezpečí materiálů/látek | Prach, kapalina, mlhovina |
| Ergonomická nebezpečí | Přístup, námaha, poloha těla, místní osvětlení atd. |
| Nebezpečí spojená s prostředím, ve kterém je stroj používán | Prach a mlhovina, elektromagnetické rušení, teplota, vlhkost |

Dále jsou zde uvedeny bezpečnostní požadavky a opatření pro odstranění nebo snížení rizik souvisejících s významnými nebezpečími. Zahrnují konkrétní požadavky týkající se návrhu hydraulických, pneumatických a elektrických systémů, bezpečnostní ochranu proti mechanickým nebezpečím, které vznikají při různých režimech provozu v nástrojové oblasti, opatření proti nebezpečí poruchy ovládacího systému nebo komponenty atd. Všechny uvedené požadavky a opatření musí být následně ověřeny. K tomu je v normě uvedena také stručná tabulka s jejich seznamem a metodami ověření. [17]

ČSN EN ISO 16092-3 upřesňuje a doplňuje všeobecné bezpečnostní požadavky uvedené v části 1. Součástí je také tabulka, ve které jsou uvedeny hlavní bezpečnostní systémy, příslušné bezpečnostní funkce, minimální $PL_r$ a základy pro návrh vstupu, logiky a výstupu bezpečnostní funkce. V přílohách normy jsou uvedeny příklady řešení bezpečnostních funkcí. [18]

# 6 BOSCH REXROTH

Bosch Rexroth je součástí společnosti Bosch Group, která je známá po celém světě výrobky z oblasti automobilové techniky, průmyslových technologií, spotřebního zboží či energetiky a vybavení budov. [19]

## 6.1 Bosch Rexroth celosvětově

V roce 1795 založil George Ludwig Rexroth ve městě Elsavatal v Německu kovárnu, jejíž součástí byl vodou poháněný buchar, a tím započala historie společnosti Bosch Rexroth. Od výroby odlitků a výkovků se firma Rexroth postupně dostala až k výrobě hydraulických komponent a v roce 1975 byla odkoupena společností Mannesmann AG, čímž vznikl Manesmann Rexroth. Ten se stal v roce 2001 součástí Bosch Rexroth AG. [19]

V současnosti se Bosch Rexroth zabývá pohony a řídícími technologiemi, jež spadají do oblasti průmyslových technologií, a jejich výrobky lze nalézt v oblastech jako jsou montážní technika, lineární technika, hydraulika (průmyslová, mobilní i kompaktní) nebo automatizace a elektrické technologie. Kromě toho se také zabývají divadelní technikou a speciálními aplikacemi, např. pro výletní loď AIDAnova byla dodávána technologie v podobě LED stěny, točny a tubusu (obr. 11). [19]

Obr. 11) Technologie pro loď AIDAnova [20]

Hlavním sídlem společnosti Bosch Rexroth je Lohr nad Mohanem (Německo) a v roce 2018 bylo zaměstnáno více než 32 tisíc pracovníků po celém světě. [19]

## 6.2 Bosch Rexroth v České republice

Historie Bosch Rexroth v České republice sahá až do roku 1990, kdy zde vznikla první dceřiná společnost Mannesmann Rexroth, a z ní v roce 2001 Bosch Rexroth, spol. s r.o. [19]

Pobočky se nachází v Praze, Brně a Ostravě zaměstnávají více než 200 pracovníků. Hlavní sídlo společnosti (obr. 12) se nachází v Brně-Černovicích a je zároveň jediným výrobním závodem Bosch Rexroth v ČR. V budově se nachází kancelářské prostory a výrobní hala se dvěma zkušebnami a lakovnou, kde jsou vyráběny převážně hydraulické agregáty a v menším množství také zkušební standy, které slouží ke zkoušení a nastavování čerpadel a ventilů, a systémy. Kromě toho se Bosch Rexroth, spol. s r.o. zaměřuje i na projekci a dodávku divadelních technologií, ať už v rámci ČR (např. Státní opera Praha nebo plzeňské Divadlo Jízdecká) nebo v zahraničí (např. Opera Krakow či Národní divadlo Bratislava), a na speciální aplikace. [19]

Vyjma výroby společnost nabízí produkty skupiny Bosch Rexroth, servisní služby, (externí montáže, opravy u zákazníka, diagnostiku aj.) a školení hydrauliky. [19]


Obr. 12) Brněnská pobočka Bosch Rexroth, spol. s r.o.

# 7 FUNKČNÍ BEZPEČNOST V BOSCH REXROTH

Společnost Bosch Rexroth vnímá bezpečnost produktů jako klíčovou pro úspěch na trhu a dbá na to, aby všechny produkty byly vyrobeny v souladu s platnou legislativou. Nabízí svým zákazníkům řešení v podobě „Safety on Board“, což zahrnuje všechny činnosti spojené se zajištěním bezpečnosti produktu – od posouzení rizik přes návrh a výrobu až po zaškolení zaměstnanců, a to včetně zajištění funkční bezpečnosti, pokud je relevantní. [21]

Bosch Rexroth se funkční bezpečností zabývá již mnoho let a patří k jedněm z předních výrobců spolehlivých bezpečnostních částí. V roce 2012 byla také vydána kniha s názvem 10 steps to performance level, jež slouží jako příručka pro zajištění funkční bezpečnosti dle ISO 13849.

Produktové portfolio Bosch Rexroth lze rozdělit do tří oblastí: komponenty, hydraulické agregáty a projekty. Těmto oblastem budou věnovány následující podkapitoly.

## 7.1 Komponenty

Jednou z důležitých oblastí působnosti Bosch Rexroth v ČR je prodej hydraulických komponent vyráběných v závodech Bosch Rexroth po celém světě. Nabídka produktů je široká a zahrnuje např. různé druhy ventilů, rozvodné bloky, čerpadla, hydromotory či řídící jednotky.

Vzhledem k rozsáhlé nabídce jsou pro komponenty relevantní dle jejich druhu a použití různé předpisy a normy. Mezi relevantní předpisy může patřit např. směrnice Evropského parlamentu a Rady 2014/68/EU o harmonizaci právních předpisů členských států týkajících se dodávání tlakových zařízení na trh či směrnice Evropského parlamentu a Rady 2006/42/ES o strojních zařízeních. Co se týče norem, jedná se např. o ISO 4413 zabývající se požadavky na hydraulické systémy a jejich součásti.

Všechny hydraulické komponenty související s bezpečností (ventily aj.) jsou navrhovány, vyráběny a testovány v souladu s normou ISO 13849 a jsou tedy vhodné pro bezpečnostní funkce. Pro každou komponentu jsou k dispozici produktové listy, kde jsou kromě základních parametrů a vlastností uvedeny také hodnoty $MTTF_D$. V případě standardizovaných rozvodných bloků je v produktovém listě uvedena přímo hodnota PL vypočtená v závislosti na zapojení a použitých prvcích. Některé bloky splňují kromě požadavků ISO 13849 také požadavky jiných norem (např. ISO 16092) v závislosti na aplikaci.

Obr. 13) Blok IH04C [22]

## 7.2 Hydraulické agregáty

Hydraulický agregát (obr. 14) slouží jako pohonná jednotka pro strojní zařízení využívající tlak kapaliny jako zdroj energie. Standardně je složen z čerpadla s elektromotorem, nádrže, filtrů, regulačních a řídících prvků, potrubí, hadic a dalších spojovacích prvků. Dle provozních požadavků a požadavků zákazníka mohou být součástí i další komponenty, např. hydraulické akumulátory, komponenty pro indikaci veličin (hladinoměry, teploměry aj.), chladiče atd. [19]

Relevantním předpisem pro bezpečnost je směrnice Evropského parlamentu a Rady 2006/42/ES o strojních zařízeních. Z pohledu této směrnice jsou hydraulické agregáty neúplná strojní zařízení, tzn. jsou určeny k zabudování do jiných strojních zařízení a nemohou fungovat samostatně. Spolu s produktem je zákazníkovi dodáno prohlášení o zabudování neúplného strojního zařízení. [23]

Centrálou Bosch Rexroth byla v roce 2015 vydána řada směrnic DCCS 06001: Principles on the Product Safety of Hydraulic Power Units. Za předpokladu splnění požadavků této řady směrnic jsou při návrhu a výrobě dodrženy i relevantní legislativní požadavky na bezpečnost. Jednotlivé části zahrnují obecné požadavky a zásady, popis metod a nástrojů pro posouzení rizik, opatření pro snížení rizik, požadavky týkající se dokumentace, požadavky na konstrukci atd. [23]

Zadání od zákazníka obvykle obsahuje pouze potřebné parametry pro návrh a výrobu hydraulického agregátu (výjimečně také komponenty, které mají být použity) a není v něm specifikováno, v jakém strojním zařízení bude používán a k jakému účelu bude konečné strojní zařízení určeno. Vzhledem k tomu, že výsledná bezpečnost strojního zařízení může být ovlivněna zapojením hydraulického agregátu do celku, není u agregátů funkční bezpečnost řešena a odpovídá za ni konečný výrobce kompletního strojního zařízení.

Obr. 14) Hydraulický agregát [33]

## 7.3 Projekty

Dodávky komplexních zařízení zahrnující celý hydraulický systém včetně řízení jsou řešeny jako projekty. Návrh a výroba zařízení tedy zahrnuje minimálně pohonnou jednotku, odpovídající akční členy (motory, válce atd.) a hydraulické/elektronické ovládání nebo PLC. Zákazníkovi je tak dodáno plně funkční zařízení, ne pouze pohonný subsystém jako v případě hydraulických agregátů. Součástí zakázky je také uvedení zařízení do provozu.

V rámci projektů jsou řešena různá zařízení, tudíž se na ně vztahují různé legislativní předpisy dle druhu zařízení a aplikace. Stejně jako u hydraulických agregátů musí být vždy splněny požadavky směrnice Evropského parlamentu a Rady 2006/42/ES o strojních zařízeních. Relevantnost předpisů nejlépe vyjadřuje tabulka č. 16, kde je uvedeno jejich porovnání pro hydraulické agregáty a projekty.

Tab 16) Relevantní předpisy pro hydraulické agregáty a projekty – porovnání [22]

P – povinné, A – záleží na aplikaci

| **Předpis** | **Název** | **Hydraulické agregáty** | **Projekty** |
|---|---|---|---|
| ČSN EN ISO 12100:2011 | Bezpečnost strojních zařízení – Všeobecné zásady pro konstrukci – Posouzení rizika a snižování rizika | P | P |
| ČSN EN ISO 13849-1:2017 | Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů - Část 1: Obecné zásady pro konstrukci | - | P |
| ČSN EN ISO 13849-2:2013 | Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 2: Ověřování platnosti | - | P |
| ČSN EN ISO 4413:2011 | Hydraulika – Všeobecná pravidla a bezpečnostní požadavky na hydraulické systémy a jejich součásti | P | P |
| 2006/42/ES | Směrnice Evropského parlamentu a Rady o strojních zařízeních | P | P |
| 2004/108/ES | Směrnice Evropského parlamentu a Rady 2004/108/ES o sbližování právních předpisů členských států týkajících se elektromagnetické kompatibility a o zrušení směrnice 89/336/EHS | A | A |
| 2014/35/EU | Směrnice Evropského parlamentu a Rady o harmonizaci právních předpisů členských států týkajících se dodávání elektrických zařízení určených pro používání v určitých mezích napětí na trh | A | A |
| 2014/34/EU | Směrnice Evropského parlamentu a Rady o harmonizaci právních předpisů členských států týkajících se zařízení a ochranných systémů určených k použití v prostředí s nebezpečím výbuchu | A | A |
| 2014/68/EU | Směrnice Evropského parlamentu a Rady o harmonizaci právních předpisů členských států týkajících se dodávání tlakových zařízení na trh | A | A |

V rámci návrhu a výroby plně funkčních zařízení musí být uvažována i funkční bezpečnost (viz předchozí tabulka č. 16). Vzhledem k tomu, že systémy zahrnují i hydraulické prvky, je pro plnění legislativních požadavků týkajících se funkční bezpečnosti využívána norma ČSN EN ISO 13849. Brněnský Bosch Rexroth aktuálně v této oblasti využívá spolupráci s externími společnostmi, což má své výhody i nevýhody.

Výhody spolupráce s externisty:

+ Projekty nejsou řešeny v pravidelných intervalech, ale pouze nárazově. Z tohoto důvodu je pro společnost ekonomicky nevýhodné zaměstnávat odborníka na funkční bezpečnost.
+ Externista má v oblasti funkční bezpečnosti odborné znalosti a bohaté zkušenosti s řešením různých aplikací.

Nevýhody spolupráce s externisty:

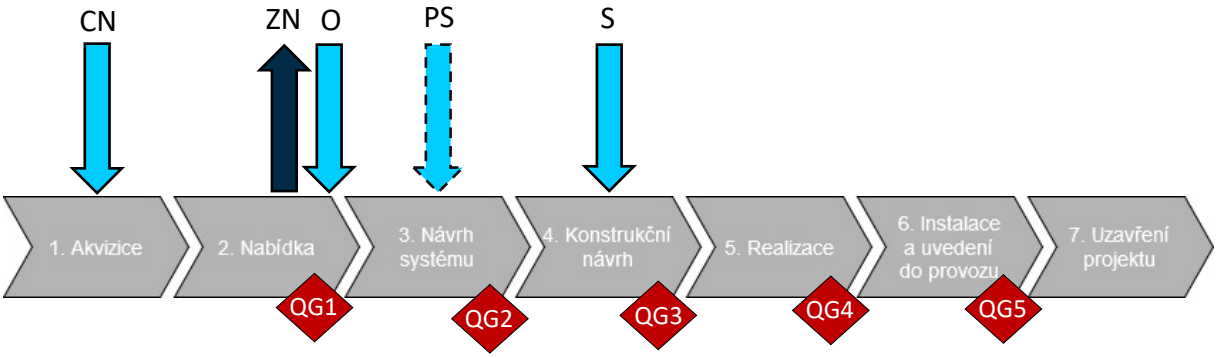
- Externista nemá přehled o produktech Bosch Rexroth a není součástí projektu již od začátku, tzn. nemá o jeho řešení celkový přehled. Problémem tak mohou být např. průběžné změny ve schématech a kusovnících, o kterých se nemusí dozvědět vůbec nebo pozdě.
- Komunikace mezi zainteresovanými stranami je složitá a časově náročná, protože mnoho pracovníků spojených s projektem nemá dostatečné povědomí o funkční bezpečnosti (např. neví, co je to PL nebo jaká dokumentace by pro řešení měla být externistovi předána).

Výstupem spolupráce s autorizovanými externisty je celkové posouzení funkční bezpečnosti navrhovaného systému, což zahrnuje výpočet PL jednotlivých bezpečnostních funkcí (obvykle v programu SISTEMA) a doporučení v případě nesplnění požadavků na funkční bezpečnost navrhovaného systému. Na základě doporučení jsou případně navržené změny implementovány a je znovu ověřeno, zda byly dostatečné.

# 8 BEZPEČNOST A PROJEKTOVÉ ŘÍZENÍ V BOSCH REXROTH

Aby mohly být v rámci projektu splněny nejenom požadavky zákazníka, ale i požadavky legislativní, je nutné se zabývat bezpečností již od samého začátku projektu, tzn. od převzetí zadání. Zanedbání bezpečnostních požadavků v rané fázi projektu může vést k tomu, že zařízení nebude možné uvést na trh. S tím jsou spojené vícenáklady vynaložené pro dodatečné splnění požadavků legislativy nutných pro uvedení na trh a prodloužení dodacího termínu. V horším případě, kdy by bylo nevyhovující zařízení uvedeno na trh, hrozí vážný dopad na zdraví osob a další právní důsledky.

Systematický a jednotný postup při řešení projektů v Bosch Rexroth je definován v centrální směrnici CD 02500: Project management at Bosch platné pro celý Bosch Group, na niž navazuje směrnice upravená pro oblast pohonných a řídících technologií DCCD 08924: Project Management at Bosch – DC specific regulations/supplement. V rámci tohoto postupu je definováno sedm fází projektu uvedených na obr. 15, jež je doplněn tabulkou č. 17 popisující stručně činnosti, které jsou v jednotlivých fázích vykonávány. Na obrázku jsou také znázorněny tzv. Quality Gates, které jsou z pohledu zajištění bezpečnosti nejdůležitějším nástrojem projektového řízení v Bosch Rexroth a bude jim věnován zbytek této kapitoly.




| | |
|---|---|
| CN – žádost o cenovou nabídku | PS – předběžné schválení zákazníkem |
| ZN – závazná nabídka | S – schválení zákazníkem |
| O – objednávka | |

Obr. 15) Fáze projektu a Quality Gates [25]

Tab 17) Příklady činností vykonávaných v jednotlivých fázích projektu [26]

| **Fáze projektu** | **Popis fáze** |
|---|---|
| Akvizice | Jedná se o fázi, kdy jsou shromažďovány informace o projektu, analyzují se legislativní požadavky a důvěryhodnost zákazníka, posuzují se rizika projektu atd. Na základě získaných informací je rozhodnuto o tom, zda bude projekt realizován či nikoliv. |
| Nabídka | Nejprve je sestaven projektový tým. Ze zadání a doplňujících informací je vytvořena specifikace, popis a návrh systému, definují se požadavky na dokumentaci, dodavatele atd. Dále je vytvořen plán projektu. Nabídková fáze končí vytvořením smlouvy a podpisem zákazníka. |
| Návrh systému | V rámci návrhu systému jsou vypracována hydraulická a elektrická schémata a předběžný kusovník se základními prvky, dle nějž jsou již objednány některé materiály. Součástí je také vývoj softwaru, pokud je relevantní. |
| Konstrukční návrh | Dle návrhu systému jsou následně vytvářeny detailní výkresy, finální kusovník a případně jsou doobjednány materiály. Kromě toho je také zpracován plán zkoušek. Relevantní dokumenty jsou předány zákazníkovi ke schválení. |
| Realizace | Realizace zahrnuje dodání materiálu a montáž jednotlivých částí zařízení do jednoho celku. Jsou vypracovány plány pro instalaci a uvedení do provozu. |
| Instalace a uvedení do provozu | Zařízení je oživeno a otestováno, aby byla zajištěna jeho správná funkčnost. Funkční zařízení je předáno zákazníkovi včetně dokumentace a zákazník je proškolen. |
| Uzavření projektu | Na závěr jsou archivovány všechny potřebné dokumenty a projekt je zhodnocen z pohledu nákladů, zákaznické spokojenosti atd. |

Quality Gates (QG) jsou specifické milníky, které jsou používány pro zajištění kvality procesu a výsledného produktu pomocí vyhodnocení dosažených výsledků na základě definovaných kritérií (bodů) a umožňují včasnou identifikaci případných odchylek od cílů a plánu projektu. Minimalizují tak riziko, že nebudou splněny požadavky legislativní nebo požadavky zákazníka. [27]

QG jsou umístěny na konci projektových fází, jak je patrné z obrázku č. 14, a splnění bodů jednotlivých QG je podmínkou pro postup do následující fáze projektu. Je tak zajištěno, že v další fázi projektu nebudou chybět potřebné informace a dokumenty. Kromě toho nelze přeskočit některou fázi projektu, čímž je zaručena systematičnost řešení projektů.

Každá QG má specifický dotazník obsahující jednotlivé body, které musí být splněny. Tyto body jsou vždy rozděleny do 7 oblastí [28]:

- odbyt, uzavírání smluv a controlling,
- projektový management a management kvality,
- návrh a konstrukce,
- kodex vývoje produktu (směrnice vydaná centrálou Bosch Group, která obsahuje požadavky týkající se legálnosti, požadované úrovně vědy a testovacích cyklů, které nesmí být rozpoznatelné),
- IT zabezpečení a SW,
- nákup, logistika a výroba,
- instalace a uvedení do provozu.

Každému bodu je přidělen status – červená (není splněno a i po realizaci opatření nebude nejméně jeden cíl projektu dosažen), žlutá (není splněno, ale po realizaci opatření budou cíle projektu dosaženy), zelená (splněno, nejsou nutná další opatření a cíle projektu budou dosaženy) nebo nerelevantní. Celkové hodnocení plnění QG se odvíjí od nejhůře hodnoceného bodu. V případě celkového zeleného nebo žlutého statusu lze začít další fázi, u červeného statusu nesmí být další fáze zahájena, dokud nebudou příslušné body splněny a status nebude vyhodnocen alespoň jako žlutý. [27]

Pro účely této diplomové práce jsou v tabulce č. 18 shrnuty pouze body, které se týkají funkční bezpečnosti.

Tab 18) Body relevantní pro funkční bezpečnost v jednotlivých QG [29]

| | **Body relevantní pro funkční bezpečnost** |
|---|---|
| **QG1** | ✓ ověření technických požadavků (dostupnost, legálnost a proveditelnost),<br>✓ vytvoření návrhu systému,<br>✓ zahájení posouzení rizik,<br>✓ zahrnutí nákladů spojených se zajištěním požadované úrovně bezpečnosti do celkové kalkulace. |
| **QG2** | ✓ finalizace návrhu systému,<br>✓ vytvoření kusovníku,<br>✓ zvážení relevantnosti CE prohlášení o shodě,<br>✓ schválení konečného návrhu. |
| **QG3** | ✓ dokončení posouzení rizik,<br>✓ zahájení vytváření návodů pro uživatele. |
| **QG4** | ✓ ověření implementace všech opatření vycházejících z posouzení rizik,<br>✓ zahájení zpracování CE prohlášení o shodě v případě, že je relevantní. |
| **QG5** | ✓ dokončení návodů k zařízení. |

Relevantnost jednotlivých QG se odvíjí od kategorizace projektu. Každý projekt může být zařazen do jedné z pěti kategorií: A, B, C, D2 nebo D1, přičemž projekty kategorie A jsou nejsložitější a D1 nejjednodušší. Kategorie je určena na základě několika kritérií týkajících se ekonomických hledisek, rizik, náročnosti, cílového trhu a unikátnosti řešení. Každé kritérium má definovanou váhu a bodové hodnocení 1-5. Pro zařazení je rozhodující celkový počet bodů. [29]

Brněnský Bosch Rexroth může řešit pouze projekty dosahující maximálně kategorie C. Relevantní QG (označeny „x“) pro tyto kategorie jsou uvedeny v tabulce 19. Projekty kategorie A a B nejsou řešeny, protože společnost pro jejich řešení nemá příslušné kompetence.

Tab 19) Vliv kategorizace projektu na Quality Gates [29]

| | **QG1** | **QG2** | **QG3** | **QG4** | **QG5** |
|---|---|---|---|---|---|
| **C** | x | x | x | x | x |
| **D1** | x | | x | x | |
| **D2** | x | | x | | |

Důvodem pro vynechávání některých QG u jednodušších projektů kategorie D1 a D2 je, že obsažené body nejsou z hlediska řešení těchto projektů relevantní. Kromě toho s těmito projekty není spojené takové riziko jako v případě složitějších projektů, a to hlavně z pohledu nákladů.

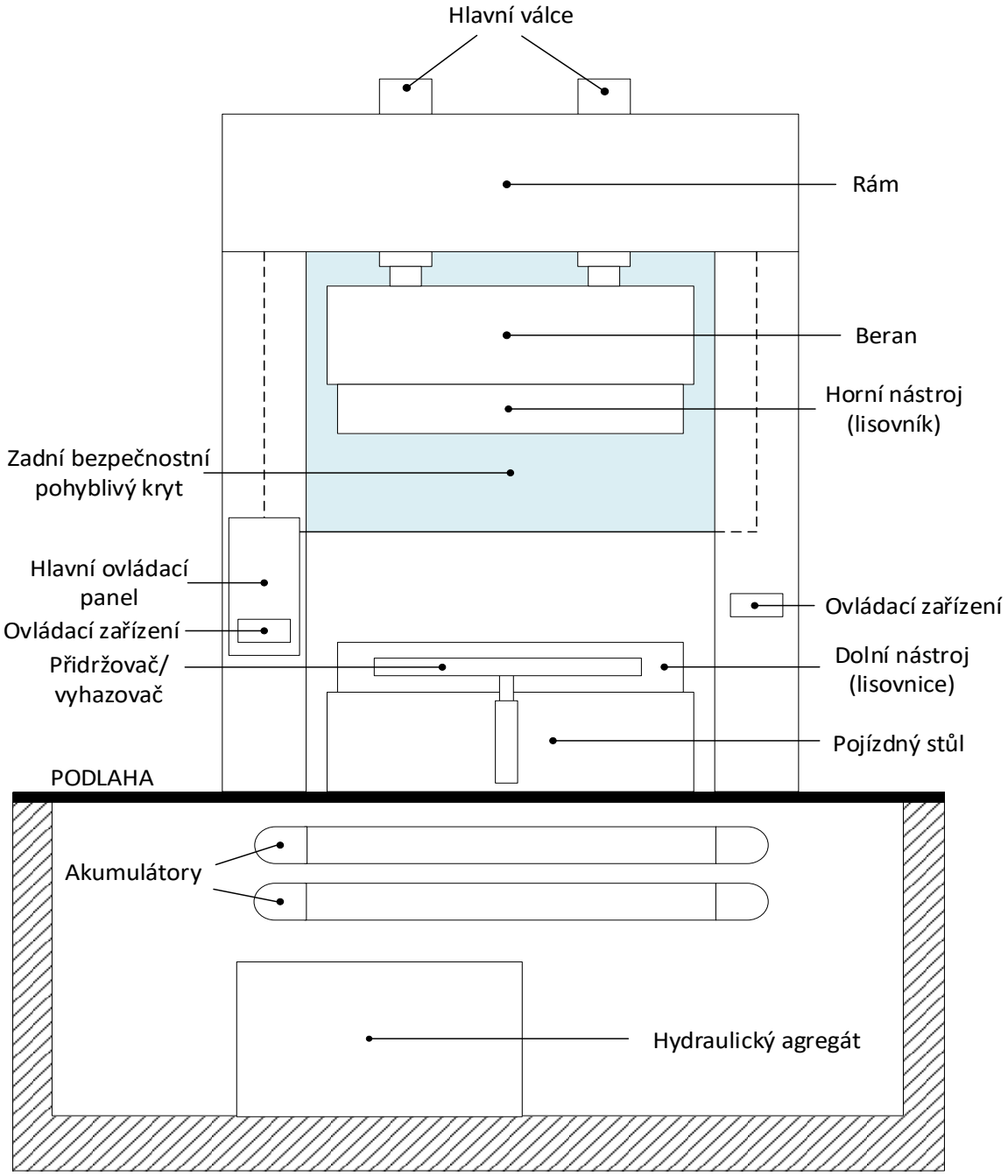
# 9 FUNKČNÍ BEZPEČNOST HYDRAULICKÉHO LISU MW2100

Lis MW2100 je hydraulický zapracovávací (zkušební) lis, který slouží k úpravě nástrojů a nastavení potřebných parametrů lisu (např. síla nebo rychlost beranu) pro tvarování dílů karoserií automobilů. Je tedy určen k odzkoušení nástroje ještě před jeho instalací a používáním v sériové výrobě. Díky tomu lze ušetřit náklady i čas spojený s odstavením lisů (obvykle klikových) v sériové výrobě kvůli výměně nástroje, a zvýšit tak produktivitu výroby.

Lis byl poprvé uveden do provozu v roce 1999. Vzhledem k průběžnému opotřebení jednotlivých částí dochází pravidelně k jejich opravám, výměnám nebo náhradám. Brněnská společnost Bosch Rexroth se podílí na opravách a výměnách hydraulických prvků a náhradě stávajícího řídicího systému za nový.

Kvůli dodržení závazku mlčenlivosti vůči zákazníkovi nelze zveřejnit fotografii zařízení, jehož funkční bezpečnost bude dále v této části řešena. Níže je tedy pro představu o tom, jak zapracovávací lis vypadá, uveden alespoň obrázek lisu od firmy Schuler, jež se řešenému zařízení velmi podobá (obr. 16). Hlavní části lisu jsou popsány na obr. 17.


Obr. 16) Zapracovávací lis od firmy Schuler [30]




Obr. 17) Schéma lisu

Lis využívá pro svoji funkci Pascalův zákon, dle nějž se tlak v kapalině šíří všemi směry stejně. Zdrojem tlakové kapaliny je hydraulický agregát, jehož hlavními částmi jsou nádrž a čerpadlo poháněné elektromotorem.

Čerpadlo slouží k převodu elektrické energie dodávané elektromotorem na energii tlakovou. Nasává pracovní kapalinu (hydraulický olej) z nádrže a plní jím hydraulický systém (ventily, rozvodné bloky atd.). Součástí hydraulického systému jsou také pístové akumulátory, což jsou tlakové nádoby, které jsou využívány jako zdroj energie v případě poruchy a k tlumení hydraulických rázů.

Přes hydraulické vedení a hydraulické prvky je tlaková kapalina dopravena až do prostoru čtyřech hlavních válců, které ovládají beran. Zde dochází k přeměně tlakové síly kapaliny na mechanickou práci (přímočarý pohyb). Na beranu je uchycen horní nástroj (lisovník).

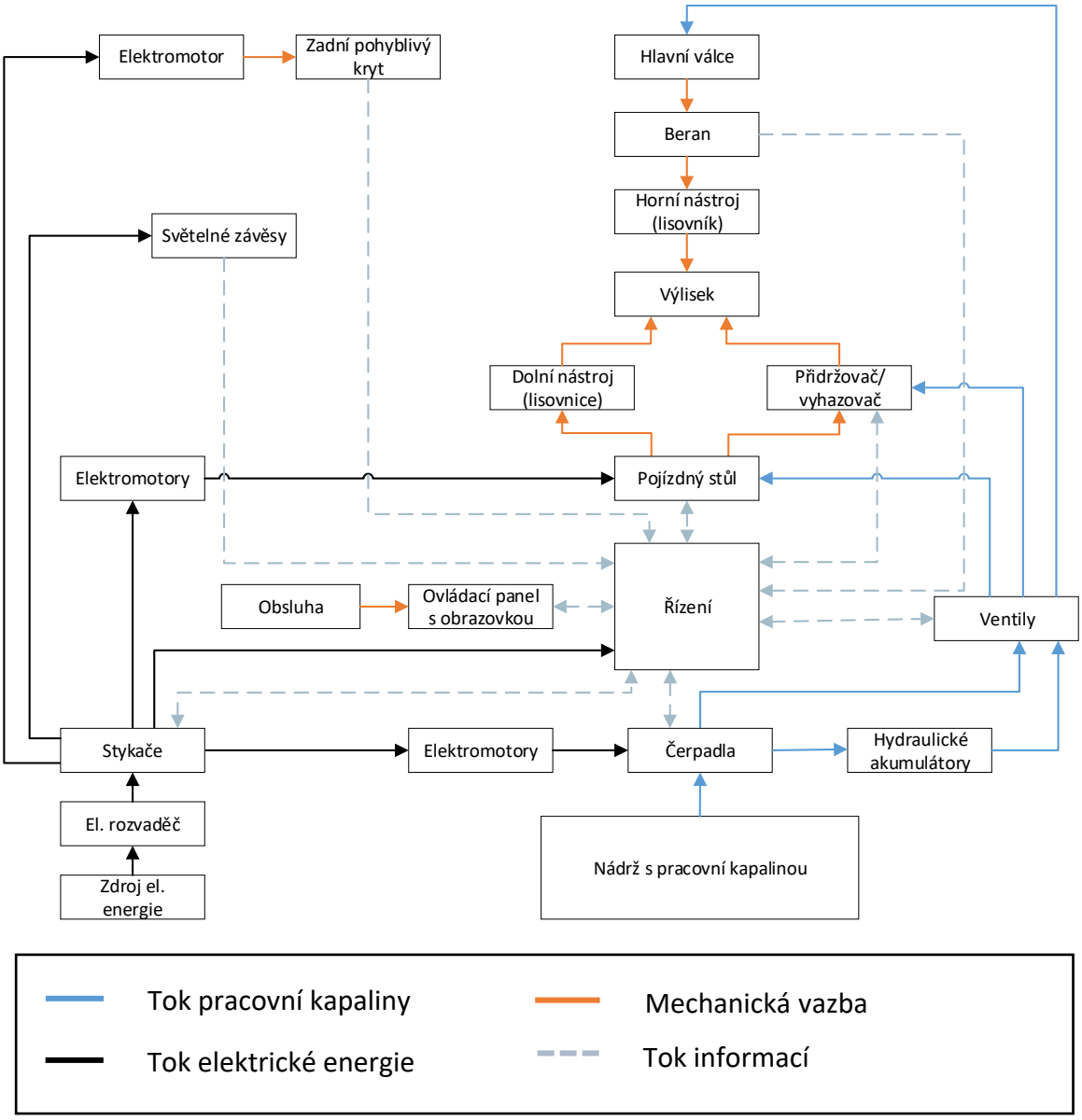
Spodní část nástroje (lisovnice) je upevněna na pojízdném stole, jež slouží k jejímu transportu a manipulaci při výměně. Pojezd stolu je realizován elektromechanicky pomocí elektromotoru poháněnjícího kola, která se pohybují v kolejnicích. Zvedání/spouštění stolu je zajištěno hydraulicky.

V pojízdném stole je zabudován hydraulicky ovládaný přidržovač, který při tváření přidržuje materiál, a zamezuje tak jeho posunutí. Kromě toho také uvolňuje nebo absorbuje sílu, čímž zamezuje vzniku deformací materiálu. Plní i funkci vyhazovače, jehož cílem je usnadnit vyjmutí výlisku po tváření.

Ovládání lisu je možné pomocí hlavního ovládacího panelu umístěného v přední levé části lisu nebo v případě automatického režimu lze využít až čtyři výklopná ovládací zařízení (dvě vpředu, dvě vzadu), přičemž jedno ovládací zařízení je součástí hlavního ovládacího panelu.

Při ovládání lisu z přední strany není možné vizuálně kontrolovat zadní část nebezpečného prostoru, proto je tento prostor vybaven pohyblivým ochranným krytem, jehož pohyb je ovládán elektromotorem. Kryt musí být spuštěn vždy před zahájením nebezpečných pohybů, a zabránit tak vstupu osob a následným zraněním. V případě, že je lis obsluhován ze zadní strany lisu, je pohyb krytu deaktivován.

Funkční schéma lisu je znázorněno na obr. 17.




Obr. 18) Funkční schéma lisu MW 2100

Zapracovávací lis MW 2100 může být provozován ve třech režimech:

- **tipování**, které slouží hlavně při údržbě a opravách, ale i pro obsluhu lisu. Ovládání je možné pouze manuálně pomocí tlačítek na hlavním ovládacím panelu. Pohyby jsou vykonávány nízkou rychlostí a bez lisovacího tlaku. Tento režim je využíván např. i po instalaci nového nástroje, kdy je potřeba zajistit, aby obě části nástroje správně navzájem dosedly.
- **seřizování**, jež je používáno výhradně obsluhou lisu. Je umožněno např. polohování beranu, nastavování rychlosti a síly beranu v závislosti na jeho poloze atd. Tento režim slouží pro zjišťování parametrů potřebných pro dosažení požadovaného tvaru dílu karoserie, tzn. seřízení nástroje, ne samotného stroje. Výsledkem je tzv. receptura, což je soubor rychlostních, silových a polohových parametrů. Ovládání je možné opět pouze pomocí tlačítek na hlavním ovládacím panelu.

- **jednotlivý zdvih** určený k provedení kompletního lisovacího cyklu dle nastavených parametrů (receptury) pro daný typ nástroje. Cyklus probíhá zcela automaticky a může být aktivován stlačením dvouručního ovládacího zařízení umístěného na čtyřech stanovištích.

Tipování a seřizování jsou režimy manuální a jednotlivý zdvih je režim automatický. Volba režimu je možná pomocí tlačítek na hlavním ovládacím panelu.

Lis může využívat pouze řádně proškolená osoba starší 18 let, která má k dispozici čip s příslušným oprávněním. Konkrétně se jedná o seřizovače, obsluhu a údržbáře a mají vždy přiřazena pouze práva související s jejich prací.

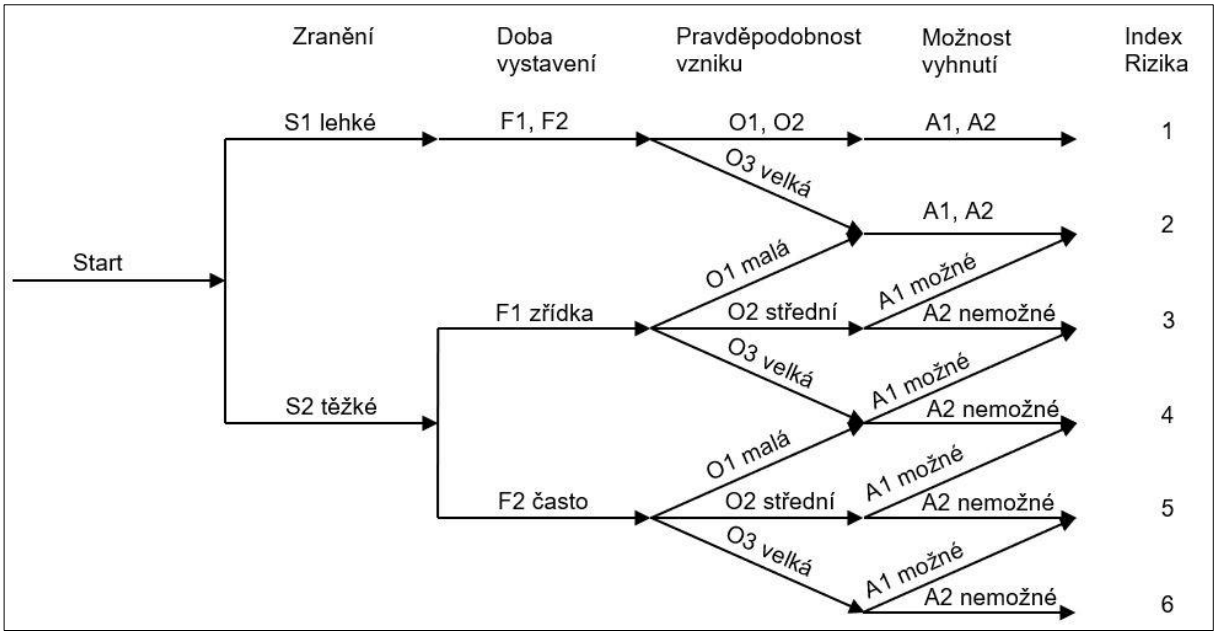
## 9.1 Posouzení rizik

Normy ČSN EN ISO 16092-1 a ČSN EN ISO 16092-3 uvádějí v přílohách A významná nebezpečí, jež vyžadují opatření pro snížení nebo odstranění rizik. Jedná se pouze o obecný seznam nebezpečí týkajících se hydraulických lisů, tudíž ne všechna nebezpečí musí být pro konkrétní typ hydraulického lisu relevantní nebo naopak jejich seznam nemusí být dostačující. Z tohoto důvodu je nutné celkové posouzení rizik konkrétního hydraulického lisu dle ČSN EN ISO 12100. Mohou tak být identifikována všechna relevantní nebezpečí – i ta, která nejsou v ČSN EN ISO 16092-1 a ČSN EN ISO 16092-3 uvedena a jsou z pohledu této normy nevýznamná.

Vzhledem k tomu, že tato práce je zaměřená na procesy a není jejím účelem provést celkové posouzení rizik, bylo provedeno pouze pro zvolenou část životního cyklu zapracovávacího lisu – konkrétně pro provoz, který je nejdůležitější částí. Provoz zahrnuje manipulaci s materiálem (plechy pro karoserie), nastavování parametrů a ovládání lisu pomocí ovládacího panelu nebo dvouručního ovládacího zařízení a úpravy nástroje (formy) pro dosažení požadovaných výsledků (broušení atd.). Použití brusek a jiných nástrojů nebylo v posouzení rizik uvažováno, protože jejich použití neovlivňuje nebezpečnost samotného lisu. Posouzení rizik je součástí přílohy 1 této práce.

Z důvodu zachování jednotné formy pro posouzení rizik u všech projektů byl nejprve navržen formulář zohledňující požadavky normy ČSN EN ISO 12100. K tomu byl využit Microsoft Excel. Ve vrchní části formuláře je hlavička se základními údaji pro identifikaci zakázky, zařízení a také autora posouzení rizik. Samotnou tabulku pro posouzení rizik lze rozdělit na dvě části. První část obsahuje identifikaci nebezpečí, tzn. druh nebezpečí, zdroj, popis, fázi životního cyklu, stav stroje a ohrožené osoby. Druhou část tvoří odhad a případné snížení rizika. Pro odhad byl doposud v Bosch Rexroth používán graf rizika vycházející z ISO/TR 14121-2 (obr. 19).

Jedná se o velice jednoduchou metodu a vzhledem k tomu, že tato metoda je ve firmě pro konstruktéry, projektové manažery a jiné zainteresované osoby všeobecně známá, je vhodné její ponechání. Jednotlivé parametry použité pro odhad a jejich popis jsou uvedeny v tabulce č. 20. Na základě zadaných parametrů je poté riziko vyhodnoceno jako vysoké (5-6), střední (3-4) nebo nízké (1-2). Aby nebylo vždy nutné hledání „cesty“ v grafu rizik, byly tyto cesty pro urychlení a zjednodušení nastaveny pomocí funkcí. Po návrhu opatření byla jednotlivá rizika opět zhodnocena.




Obr. 19) Graf rizik dle ISO/TR 14121-2

Tab 20) Parametry pro odhady rizik dle ISO/TR 14121-2 [31]

| **Parametr** | | **Popis** |
|---|---|---|
| Závažnost zranění (S) | 1 | Lehké zranění (obvykle bez následků), např. škrábance, modřiny či zranění vyžadující první pomoc; neschopnost vykonávat stejný úkol po dobu kratší než 2 dny |
| | 2 | Těžké zranění (obvykle s následky), např. zlomeniny, zranění vyžadující stehy či amputace končetin; neschopnost vykonávat stejný úkol trvá déle než 2 dny |
| Četnost a/nebo doba vystavení nebezpečí (F) | 1 | Výjimečné až poměrně časté a/nebo krátké vystavení se nebezpečí, tzn. dvakrát nebo méně za pracovní směnu a/nebo celkově méně než 15 minut za pracovní směnu |
| | 2 | Časté až nepřetržité a/nebo dlouhé vystavení se nebezpečí, tzn. více než dvakrát za pracovní směnu a/nebo celkově více než 15 minut za pracovní směnu |
| Pravděpodobnost výskytu nebezpečné události (O) | 1 | Nízké – použití robustní a moderní technologie osvědčené v bezpečnostních aplikacích |
| | 2 | Střední – v posledních dvou letech došlo jednou k poruše, obsluha má více než šest měsíců zkušeností |
| | 3 | Vysoké – k poruše dochází každých šest měsíců nebo méně, obsluha má méně než šest měsíců zkušeností |
| Možnost vyvarování se nebezpečí (A) | 1 | Možné za určitých okolností – rychlost pohybujících se částí je menší než 0,25 $m.s^{-1}$, pracovník je seznámen s riziky a je schopen v případě potřeby reagovat na vzniklá nebezpečí |
| | 2 | Nemožné |

Z posouzení rizik je patrné, že největším problémem jsou mechanická nebezpečí plynoucí z pohybujících se prvků (beran, vyhazovač/přidržovač a pohyblivý ochranný kryt) a rotujících prvků (spojky, části čerpadel a elektromotorů atd.) a dále z vysokého tlaku spojeného s použitím hydraulického systému jako zdroje energie. U všech uvedených nebezpečí je riziko vysoké.

Kromě mechanických nebezpečí bylo vysoké riziko zjištěno také u nebezpečí spojených s elektrickým systémem (zkrat, kontakt s živými částmi a elektromagnetické/elektrostatické jevy) a u hluku způsobeným pohybujícími se částmi (čerpadla a motory). Souhrn nebezpečí s vysokým rizikem je uveden v tabulce 21.

Tab 21) Nebezpečí s vysokým rizikem

| **Id. č.** | **Popis nebezpečí** | **Počát. riziko** |
|---|---|---|
| 1.1.1 | Nebezpečí vymrštění hydraulických prvků, které jsou pod tlakem | 6 |
| 1.2.1 | Nebezpečí pádu vrchní části nástroje na osobu v důsledku špatného upevnění při výměně nástroje | 6 |
| 1.2.2 | Nebezpečí pádu zadního pohyblivého ochranného krytu na osobu | 6 |
| 1.3.1 | Nebezpečí stlačení osoby při pomalém klesání beranu vlivem poruchy hydraulického, elektrického nebo mechanického systému (porucha, která nezpůsobí okamžitý pád beranu, např. postupná ztráta tlaku poruchou ventilu způsobená zanesením) | 5 |
| 1.3.2 | Nebezpečí stlačení osoby při nečekaném klesání (pádu) beranu vlivem poruchy hydraulického, elektrického nebo mechanického systému | 6 |
| 1.4.1 | Nebezpečí vystříknutí hydraulického oleje | 6 |
| 1.4.2 | Nebezpečí zasažení osoby unikajícím dusíkem z hydraulického akumulátoru | 6 |
| 1.5.1 | Nebezpečí stlačení osoby při pohybu beranu směrem dolů (vstup osoby do pracovního prostoru) | 6 |
| 1.5.2 | Nebezpečí stlačení části končetiny ve vedení beranu (vstup osoby do pracovního prostoru) | 5 |
| 1.5.5 | Nebezpečí stlačení části osoby při pohybu vyhazovače (stlačení mezi vyhazovač a beran) – vstup osoby do pracovního prostoru | 6 |
| 1.5.6 | Nebezpečí stlačení osoby při pohybu zadního pohyblivého krytu | 6 |
| 1.6.1 | Nebezpečí zachycení/vtažení části osoby rotujícími prvky (např. spojky) | 5 |
| 2.1.1 | Nebezpečí poruchy řídicího systému | 5 |
| 2.2.1 | Nebezpečí požáru | 5 |
| 2.3.1, 2.4.1 | Nebezpečí zásahu elektrickým proudem a následné popálení/smrt | 5 |
| 4.2.2 | Nebezpečí trvalého poškození sluchu v důsledku nadměrného hluku (čerpadla atd.) | 5 |

Pro snížení rizik byla využita tříkroková metoda, pomocí níž byla rizika snížena na nízkou úroveň. Jak již bylo zmíněno v kapitole 4, tříkroková metoda spočívá v postupném snižování rizik, a to nejprve pomocí konstrukčních opatření. Pokud nejsou dostačující, je nutné použít bezpečnostní ochranu a doplňková bezpečnostní opatření. V případě, že stále není dosaženo požadované úrovně rizika, musí být uživatel informován o zbytkových rizicích.

## 9.2 Bezpečnostní funkce a jejich popis

V rámci posouzení rizik pro provoz lisu bylo identifikováno několik technických bezpečnostních ochran určených pro realizaci bezpečnostních funkcí (bezpečnostní světelné závěsy, dvouruční ovládací zařízení, souhlasné povelové zařízení atd.). Na základě posouzení rizik a uvedených opatření byly zvoleny dvě bezpečnostní funkce (tabulka 22), pomocí nichž bude ukázán postup výpočtu PL.

Tab 22) Vybrané bezpečnostní funkce

| Id. číslo nebezpečí | Bezpečnostní ochrana | Bezpečnostní funkce | Režim |
|---|---|---|---|
| 1.5.1, 1.5.2, 1.5.3, 1.5.4, 1.5.5, 1.5.6, 1.6.1 | Tlačítka nouzového zastavení | Funkce nouzového zastavení realizovaná odpojením hlavních stykačů | Všechny |
| 1.5.1, 1.5.2 | Bezpečnostní světelné závěsy | Funkce bezpečného zastavení pohybu beranu iniciovaná pomocí světelných závěsů | Všechny |

### 9.2.1 Funkce nouzového zastavení realizovaná odpojením hlavních stykačů

Nouzové zastavení je funkce, která může při včasném použití odvrátit nebezpečnou situaci nebo alespoň snížit její následky zastavením zařízení. Musí fungovat jako zastavení kategorie 0 nebo kategorie 1. Zastavení kategorie 0 způsobí, že je zařízení okamžitě odpojeno od zdroje energie, přičemž mohou být potřebná dodatečná brzdící zařízení, např. pro zastavení motoru. U kategorie 1 je přívod energie zachován, avšak pouze po nutně nezbytnou dobu, než dojde k zastavení, a poté je přerušen. Vyvolaný stav musí být zachován až do ručního resetování. [32]

Pro iniciaci nouzového zastavení jsou používány ovladače, které mohou mít několik podob, např. tlačítka, dráty, lanka či tyče. Vždy musí být zbarveny červeně, a pokud je to možné, pozadí musí být žluté. [32]

Nouzové zastavení je doplňující ochranné opatření a není určeno jako primární prostředek k omezení rizika. Nelze ho ani používat k běžnému zastavení stroje. [32]

U lisu MW2100 bude popsáno nouzové zastavení kategorie 0 iniciované stisknutím tlačítka, které odpojí hlavní stykače od zdroje energie, viz tabulka 23.

Tab 23) Popis funkce nouzového zastavení realizované odpojením hlavních stykačů

| | |
|---|---|
| **Nebezpečná situace** | Ohrožení osoby nebezpečnými pohyby (beran, vyhazovač, pojízdný stůl, pohyblivý kryt, rotující součásti). |
| **Spouštěcí událost** | Zmáčknutí tlačítka pro nouzové zastavení. |
| **Reakce** | Dojde k odpojení hlavních stykačů KM300 a KM301, které zajišťují přívod elektrické energie všech částí lisu. V provozu zůstává pouze řídící jednotka, aby bylo možné sledovat stav zařízení. |
| **Bezpečný stav** | Všechny nebezpečné pohyby jsou okamžitě zastaveny, dokud nedojde k resetování. |
| **$PL_r$ dle ČSN EN ISO 16092-3** | c |

### 9.2.2 Funkce bezpečného zastavení pohybu beranu iniciovaná pomocí světelných závěsů

Jedná se o funkci, která v případě potřeby musí uvést zařízení co nejdříve do bezpečného stavu, aby nedošlo ke zranění osob. Může být na rozdíl od funkce nouzového zastavení realizována kromě zastavení kategorie 0 a kategorie 1 také jako zastavení kategorie 2, kdy nedochází k odpojení přívodu energie. V případě lisu MW 2100 se jedná o funkci zastavení kategorie 0, kdy je ihned zamezeno přívodu tlakové energie do oblasti pístů, které zajišťují pohyb beranu.

Obecně může být pro iniciaci bezpečného zastavení využito jakékoliv bezpečnostní zařízení. U této funkce jsou využity bezpečnostní světelné závěsy. Jedná se o aktivní optoelektronické ochranné zařízení (AOPD), které detekuje přítomnost osoby nebo její části (příp. objektu) pomocí paprsků. Paprsky snímají plošně prostor mezi vysílačem a přijímačem a v případě jejich přerušení je stroj uveden do bezpečného stavu. Důležitým parametrem je schopnost detekce (rozlišení), což je nejmenší průměr tělesa, který ještě může být detekován. Dle normy ČSN EN ISO 16092-1 musí být schopnost detekce u lisu menší nebo rovna 30 mm.

Stručný popis bezpečnostní funkce je uveden v tabulce č. 24.

Tab 24) Popis funkce bezpečného zastavení pohybu beranu iniciované pomocí světelných závěsů

| | |
|---|---|
| **Nebezpečná situace** | Stlačení osoby nebo její části při pohybu beranu směrem dolů. |
| **Spouštěcí událost** | Přerušení paprsků bezpečnostních světelných závěsů. |
| **Reakce** | Odtlakování prostoru nad čtyřmi písty, které zajišťují pohyb beranu, a následné zabrzdění pohybu pístů uzavřením kapaliny v prostoru pod nimi. |
| **Bezpečný stav** | Pohyb beranu je zastaven. |
| **$PL_r$ dle ČSN EN ISO 16092-3** | e |

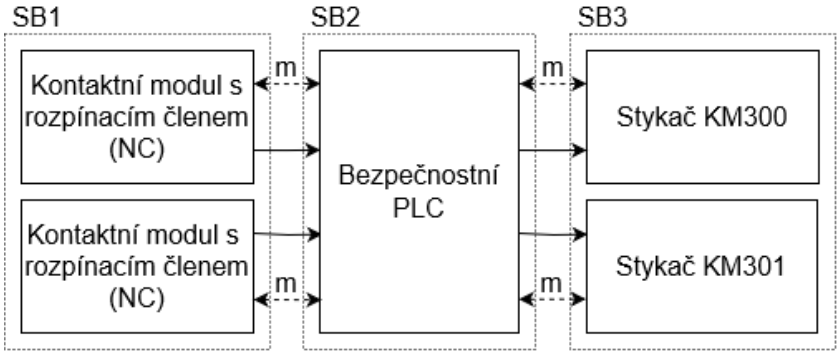
## 9.3 Návrh bezpečnostních funkcí

Při vytváření blokových schémat je nutné vzít v potaz hodnotu $PL_r$, na základě níž by měla být určena kategorie potřebná pro její dosažení. Minimální požadavek na kategorii může být dán normou typu C spolu s $PL_r$ nebo je možné využít graf na obr. 8. Díky známé kategorii lze totiž již při návrhu bezpečnostní funkce využít informace o potřebné úrovni $MTTF_D$ při volbě jednotlivých prvků, o DC zohledňující nutnost monitorování, zkoušek nebo jiných diagnostických prostředků nebo o opatřeních proti poruchám se společnou příčinou, příp. další relevantní informace týkající se dané kategorie.

### 9.3.1 Funkce nouzového zastavení realizovaná odpojením hlavních stykačů

V případě nouzového zastavení je v normě ČSN EN ISO 16092-3 uveden minimální požadavek na $PL_r$ = c a kategorii 1 pro vstup, logiku a výstup. U kategorie 1 je vyžadováno $MTTF_D$ = dlouhá, $DC_{avg}$ = žádné a CCF není relevantní.

Funkce nouzového zastavení je spuštěna pomocí tlačítka nouzového zastavení skládajícího se ze dvou kontaktních modulů, z nichž každý má jeden rozpínací člen, který je v normálním stavu sepnut (NC = normaly closed). Signál od kontaktů je předán do bezpečnostního PLC složeného z bezpečnostního vstupního modulu (SDI), procesoru (CPU) a bezpečnostního výstupního modulu (SDO). Na základě pokynu od bezpečnostního PLC dojde k odpojení hlavních stykačů KM300 a KM301. Pro zastavení všech nebezpečných pohybů je dostačující odpojení alespoň jednoho stykače. Blokové schéma funkce nouzového zastavení je zobrazeno na obr. 20.




Obr. 20) Blokové schéma funkce nouzového zastavení realizované odpojením hlavních stykačů

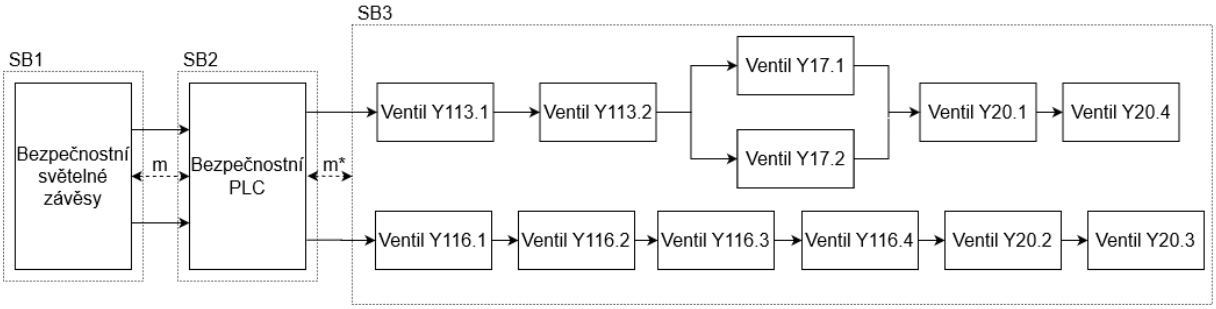
### 9.3.2 Funkce bezpečného zastavení pohybu beranu iniciovaná pomocí světelných závěsů

Zastavení pomocí AOPD musí dle normy ČSN EN ISO 16092-3 plnit $PL_r$ = e a vstup, logika a výstup musí odpovídat požadavkům kategorie 4. Je tedy vyžadováno $MTTF_D$ = dlouhá, $DC_{avg}$ = vysoké a musí být implementována opatření proti CCF.

Jako vstupní zařízení byly zvoleny světelné závěsy od společnosti SICK s rozlišením 30 mm a výrobce u nich deklaruje splnění požadavků kategorie 4 a PL = e.

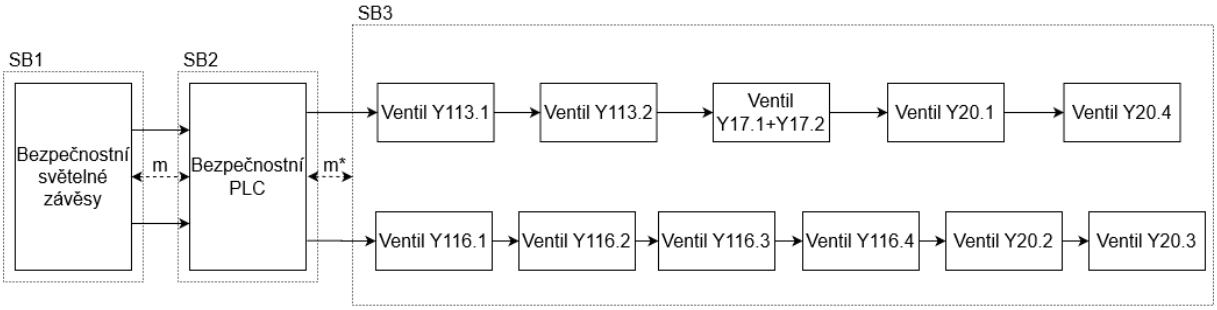
V případě, že jsou paprsky přerušeny, výstupní snímací prvky OSSD1 a OSSD2 vyšlou signál do bezpečnostního PLC, které se rovněž skládá z bezpečnostního vstupního modulu (SDI), procesoru (CPU) a v tomto případě tří bezpečnostních výstupních modulů (SDO) vzhledem k počtu ventilů a zapojení senzorů polohy na příslušné moduly dle elektrického schématu.

Pro zastavení beranu je nutné nejprve odvést tlak z prostorů nad písty ve válcích, což je realizováno propojením tlakové větve do nádrže. To lze zajistit dvěma způsoby. Prvním z nich je přepnutím ventilů Y113.1 a Y113.2 a poté alespoň jednoho z ventilů Y17.1 a Y17.2. Druhým způsobem je přepnutím čtyř ventilů Y116.1, Y116.2, Y116.3 a Y116.4. Dále je nutno zabrzdit beran zablokováním hydraulické kapaliny v prostoru pod písty, což je realizováno uzavřením ventilů Y20.1 nebo Y20.2 a zároveň Y20.4 nebo Y20.3. Základní blokové schéma funkce je znázorněno na obr. 21. Pro účely výpočtů jej lze zjednodušit spojením ventilů Y17.1 a Y17.2 v jeden blok Y17.1+Y17.2. Zjednodušené schéma znázorňuje obrázek č. 22.




∗ všechny ventily v SB3 jsou vybaveny monitorováním polohy; pro lepší přehlednost je monitorování zakresleno mezi bezpečnostním PLC a celým SB3

Obr. 21) Bezpečnostní blokové schéma funkce bezpečného zastavení pohybu beranu iniciovaná pomocí světelných závěsů




∗ všechny ventily v SB3 jsou vybaveny monitorováním polohy; pro lepší přehlednost je monitorování zakresleno mezi bezpečnostním PLC a celým SB3

Obr. 22) Bezpečnostní blokové schéma funkce bezpečného zastavení pohybu beranu iniciovaná pomocí světelných závěsů po zjednodušení

## 9.4 Výpočet PL

Bezpečnostní funkce se obvykle skládají z několika subsystémů (SRP/CS). Pro každý subsystém je nutné určit $MTTF_D$ jednoho kanálu a $DC_{avg}$ dle vzorců uvedených v kapitole 5.2 této práce. Na základě těchto hodnot lze poté pro jednotlivé subsystémy získat hodnoty $PFH_D$ a PL z tabulky K.1 normy ČSN EN ISO 13849-1. V případě certifikovaných bezpečnostních komponent je hodnota $PFH_D$ a PL obvykle uvedena v produktovém listě a nejsou nutné další výpočty.

Pro výpočet celkového $PFH_{D,BF}$ bezpečnostní funkce pak platí, že je roven součtu $PFH_D$ jednotlivých subsystémů, což lze vyjádřit pomocí vzorce č. 7. [13]

$$\mathrm{PFH_{D,BF}} = \sum_{i=1}^{n} \mathrm{PFH_{D,}}_i \tag{7}$$

Na základě $PFH_{D,BF}$ lze nakonec opětovným použitím tabulky K.1 určit PL dané bezpečnostní funkce. To však nemůže být vyšší než nejnižší PL každého subsystému a musí být v souladu s tabulkou 5 této práce. [13]

Pro ověření získaných PL bude použit volně dostupný software SISTEMA (Safety Integrity Software Tool for the Evaluation of Machine Applications) od německé společnosti IFA, který byl vyvinut v souladu s požadavky ISO 13849 a slouží jako podpora pro pracovníky, kteří se zabývají návrhem SRP/CS. Umožňuje vytvoření struktury bezpečnostní funkce a automatické provádění výpočtů na definované úrovni. Jedná se tak o velice přínosný nástroj, který uživatelům usnadňuje návrh a ověření bezpečnostních funkcí.

### 9.4.1 Funkce nouzového zastavení realizovaná odpojením hlavních stykačů

Konkrétní komponenty a hodnoty relevantní pro výpočet PL jsou shrnuty v tabulce č. 25.

Tab 25) Komponenty a hodnoty pro výpočet PL funkce nouzového zastavení realizované odpojením hlavních stykačů

| **Komponenta** | **Výrobce** | **Označení** | **Hodnoty** |
|---|---|---|---|
| Kontaktní moduly s rozpínacím členem (NC) | Siemens | 3SU1400-1AA10-1CA0 | $B_{10D}$ = 100 000 cyklů |
| | | | $n_{op}$ = 312 cyklů/rok |
| | | | DC = 99 % |
| Bezpečnostní PLC | Bosch Rexroth | Bezpečnostní vstupní modul (SDI): S20-PSDI-8/4 | $PFH_D = 1{\cdot}10^{-9}\ h^{-1}$ |
| | | | PL = e, kategorie 4 |
| | | Procesor (CPU): CFL01.1-F1 | $PFH_D = 3{,}9{\cdot}10^{-9}\ h^{-1}$ |
| | | | PL = e, kategorie 4 |
| | | Bezpečnostní výstupní modul (SDO): S20-PSDO-8/3 | $PFH_D = 1{\cdot}10^{-9}\ h^{-1}$ |
| | | | PL = e, kategorie 4 |
| Stykače KM300 a KM301 | Siemens | 3RT2024-1BB40 | $B_{10}$ = 1 000 000 cyklů |
| | | | $n_{op}$ = 624 cyklů/ rok |
| | | | DC = 99 % |

*Subsystém SB1*

$MTTF_D$ obou kontaktních modulů:

$$\mathrm{MTTF_{D,M1}} = \mathrm{MTTF_{D,M2}} = \frac{B_{10D}}{0{,}1 \cdot n_{op}} = \frac{100\,000}{0{,}1 \cdot 312} = 3\,205 \text{ roků}$$

$MTTF_D$ jednoho kanálu:

$$\mathrm{MTTF_{D,SB1,k1}} = \mathrm{MTTF_{D,S1,k2}} = \mathrm{MTTF_{D,M1}} = \mathrm{MTTF_{D,M2}} = 3\,205 \text{ roků}$$

$DC_{avg}$:

$$\mathrm{DC_{avg,SB1}} = \frac{\frac{\mathrm{DC_1}}{\mathrm{MTTF_{D1}}} + \frac{\mathrm{DC_2}}{\mathrm{MTTF_{D2}}} + \cdots + \frac{\mathrm{DC_N}}{\mathrm{MTTF_{DN}}}}{\frac{1}{\mathrm{MTTF_{D1}}} + \frac{1}{\mathrm{MTTF_{D2}}} + \cdots + \frac{1}{\mathrm{MTTF_{DN}}}} = \frac{2 \cdot \frac{0{,}99}{3\,205}}{2 \cdot \frac{1}{3\,205}} = 0{,}99 = 99\,\%$$

Tabulka č. 26 uvádí opatření proti CCF, která jsou pro subsystém SB1 relevantní.

Tab 26) Opatření proti CCF pro subsystém SB1

| **Opatření proti CCF** | **Body** |
|---|---|
| Fyzické oddělení mezi jednotlivými dráhami signálu. | 15 |
| Ochrana proti přepětí, přetlaku, nadproudu, nadteploty, atd. | 15 |
| Jsou použity osvědčené komponenty. | 5 |
| Zácvik konstruktérů za účelem pochopení příčin a následků poruch se společnou příčinou. | 5 |
| Pro elektrické/elektronické systémy zabránění kontaminace a elektromagnetická kompatibilita (EMC) k ochraně proti poruchám se společnou příčinou v souladu s příslušnými normami. | 25 |
| Byly uvažovány požadavky na odolnost proti všem relevantním vlivům prostředí, např. teplota, rázy, vibrace, vlhkost (např. tak, jak je specifikováno v relevantních normách). | 10 |

$MTTF_D$ jednoho kanálu je dlouhá, $DC_{avg}$ je vysoké a požadavky na opatření proti CCF jsou splněny. Jednotlivá závada v jakékoliv bezpečnostní části nevede ke ztrátě bezpečnostní funkce a je detekována při nebo před nejbližšími požadovanými bezpečnostními funkcemi. Subsystém tedy plní požadavky na kategorii 4 a dle tabulky K.1 je $PL_{SB1}$ = e a $PFH_{D,SB1} = 9{,}06 \cdot 10^{-10}$ $h^{-1}$.

*Subsystém SB2*

$PFH_{D,SB2}$ subsystému:

$$\mathrm{PFH_{D,SB2}} = \mathrm{PFH_{D,SDI}} + \mathrm{PFH_{D,CPU}} + \mathrm{PFH_{D,SDO}}$$

$$\mathrm{PFH_{D,SB2}} = 1 \cdot 10^{-9} + 3{,}9 \cdot 10^{-9} + 1 \cdot 10^{-9} = 5{,}9 \cdot 10^{-9}\ \mathrm{h^{-1}}$$

Všechny prvky jsou certifikované komponenty, u nichž výrobce deklaruje splnění požadavků kategorie 4 a PL = e. Výsledná hodnota $PFH_{D,SB2}$ rovněž odpovídá PL = e. Na subsystém se tedy nevztahují žádná omezení a $PL_{SB2}$ = e.

*Subsystém SB3*

Subsystém SB3 má podobnou architekturu jako SB1. Opět se jedná o dvoukanálový subsystém, přičemž každý kanál je tvořen jedním stykačem. Oba stykače jsou stejné.

$MTTF_D$ obou stykačů:

$$\mathrm{MTTF_{D,KM300}} = \mathrm{MTTF_{D,KM301}} = \frac{2 \cdot B_{10}}{0{,}1 \cdot n_{op}} = \frac{2 \cdot 1\,000\,000}{0{,}1 \cdot 624} = 32\,051 \text{ roků}$$

$MTTF_D$ jednoho kanálu:

$$\mathrm{MTTF_{D,SB3,k1}} = \mathrm{MTTF_{D,S5,k2}} = \mathrm{MTTF_{D,KM300}} = \mathrm{MTTF_{D,KM301}} = 32\,051 \text{ roků}$$

$DC_{avg}$:

$$\mathrm{DC_{avg,SB3}} = \frac{\frac{\mathrm{DC_1}}{\mathrm{MTTF_{D1}}} + \frac{\mathrm{DC_2}}{\mathrm{MTTF_{D2}}} + \cdots + \frac{\mathrm{DC_N}}{\mathrm{MTTF_{DN}}}}{\frac{1}{\mathrm{MTTF_{D1}}} + \frac{1}{\mathrm{MTTF_{D2}}} + \cdots + \frac{1}{\mathrm{MTTF_{DN}}}} = \frac{2 \cdot \frac{0{,}99}{32\,051}}{2 \cdot \frac{1}{32\,051}} = 0{,}99 = 99\,\%$$

Opatření proti CCF pro subsystém SB3 jsou shrnuty v tabulce č. 27.

Tab 27) Opatření proti CCF pro subsystém SB3

| **Opatření proti CCF** | **Body** |
|---|---|
| Fyzické oddělení mezi jednotlivými dráhami signálu. | 15 |
| Ochrana proti přepětí, přetlaku, nadproudu, nadteploty, atd. | 15 |
| Jsou použity osvědčené komponenty. | 5 |
| Zácvik konstruktérů za účelem pochopení příčin a následků poruch se společnou příčinou. | 5 |
| Pro elektrické/elektronické systémy zabránění kontaminace a elektromagnetická kompatibilita (EMC) k ochraně proti poruchám se společnou příčinou v souladu s příslušnými normami. | 25 |
| Byly uvažovány požadavky na odolnost proti všem relevantním vlivům prostředí, např. teplota, rázy, vibrace, vlhkost (např. tak, jak je specifikováno v relevantních normách). | 10 |

Subsystém SB3 splňuje požadavky na kategorii 4, protože $MTTF_D$ jednoho kanálu je dlouhá, $DC_{avg}$ vysoké a požadavky na opatření proti CCF byly splněny, závada v jakékoliv bezpečnostní části nevede ke ztrátě bezpečnostní funkce a je detekována při nebo před nejbližšími požadovanými bezpečnostními funkcemi. Z tabulky K.1 je zřejmé, že $PL_{SB3}$ = e a $PFH_{D,SB3} = 9{,}06 \cdot 10^{-10}\ h^{-1}$.

*Celkové $PFH_{D,BF1}$ a PL*

Tabulka č. 28 uvádí všechny důležité informace získané na základě výpočtů nebo od výrobce, které jsou relevantní pro výpočet $PFH_{D,BF1}$ a stanovení PL.

Tab 28) Shrnutí hodnot pro výpočet $PFH_D$ u BF1

| **Subsystém** | **$MTTF_D$ [roky]** | **DC [%]** | **Kat.** | **PL** | **$PFH_D$ [$h^{-1}$]** |
|---|---|---|---|---|---|
| SB1 | 3 205 | 99 | 4 | e | $9{,}06 \cdot 10^{-10}$ |
| SB2 | - | - | 4 | e | $5{,}9 \cdot 10^{-9}$ |
| SB3 | 32 051 | 99 | 4 | e | $9{,}06 \cdot 10^{-10}$ |

$$\mathrm{PFH_{D,BF1}} = \sum_{i=1}^{n} \mathrm{PFH_{D},}_{i} = 9{,}06 \cdot 10^{-10} + 5{,}9 \cdot 10^{-9} + 9{,}06 \cdot 10^{-10}$$

$$\mathrm{PFH_{D,BF1}} = 7{,}71 \cdot 10^{-9}\ \mathrm{h^{-1}}$$

Dle tabulky K.1 hodnotě $\mathrm{PFH_{D,BF1}} = 7{,}71 \cdot 10^{-9}\ \mathrm{h^{-1}}$ odpovídá PL = e. Všechny subsystémy dosahují úrovně e a $\mathrm{PFH_{D,BF1}}$ souhlasí i s údaji uvedenými v tabulce 5. Výsledná úroveň bezpečnostní funkce nouzového zastavení realizovaná odpojením hlavních stykačů tedy dosahuje $PL_{SF1}$ = e a jsou tak splněny požadavky na $PL_r$ = c. Ověření výsledků pomocí programu SISTEMA je uvedeno v příloze 2.

Pro splnění požadavků na $PL_r$ = c by bylo dostatečné použití pouze subsystémů odpovídajících kategorii 1, jak uvádí ČSN EN ISO 16092-1. Z výsledků je patrné, že navrhovaná funkce splňuje mnohem vyšší požadavky. Obecně z ekonomického pohledu může být tato situace nežádoucí, avšak v tomto případě byla funkce realizována pomocí standardních komponent, jejichž cena téměř neovlivní cenu celého zařízení. Díky minimálnímu zvýšení nákladů lze tak výrazně snížit pravděpodobnost nebezpečné poruchy.

### 9.4.2 Funkce bezpečného zastavení pohybu beranu iniciovaná pomocí světelných závěsů

Použité komponenty včetně hodnot relevantních pro výpočet PL uvádí tabulka č. 29.

Tab 29) Komponenty a hodnoty pro výpočet PL funkce bezpečného zastavení pohybu beranu iniciovaná pomocí světelných závěsů

| **Prvek** | **Výrobce** | **Označení** | **Hodnoty** |
|---|---|---|---|
| Světelné závěsy | SICK | C4C-EA18030A10000 | $PFH_D = 3{,}7 \cdot 10^{-9}\ h^{-1}$<br>PL = e, kategorie 4 |
| Bezpečnostní PLC | Bosch Rexroth | Bezpečnostní vstupní modul (SDI):<br>S20-PSDI-8/4 | $PFH_D = 1 \cdot 10^{-9}\ h^{-1}$<br>PL = e, kategorie 4 |
| | | Procesor (CPU):<br>CFL01.1-F1 | $PFH_D = 3{,}9 \cdot 10^{-9}\ h^{-1}$<br>PL = e, kategorie 4 |
| | | Bezpečnostní výstupní modul (SDO):<br>S20-PSDO-8/3 | $PFH_D = 1 \cdot 10^{-9}\ h^{-1}$<br>PL = e, kategorie 4 |
| Ventily s hlídáním polohy Y113.1, Y113.2, Y116.1, Y116.2, Y116.3, Y116.4 | Bosch Rexroth | Z4WE 6 X163-3X/EG24K4QSAG24WSO67 | $MTTF_D$ = 1200 let<br>DC = 99 % |
| Ventily s hlídáním polohy Y17.1, Y17.2, Y20.1, Y20.2, Y20.3, Y20.4 | Bosch Rexroth | 4WE 6 GA6X/EG24N9K4QM0G24 | $MTTF_D$ = 1200 let<br>DC = 99 % |

*Subsystém SB2*

$PFH_{D,SB2}$ subsystému:

$$PFH_{D,SB2} = PFH_{D,SDI} + PFH_{D,CPU} + 3 \cdot PFH_{D,SDO}$$

$$PFH_{D,SB2} = 1 \cdot 10^{-9} + 3{,}9 \cdot 10^{-9} + 3 \cdot 1 \cdot 10^{-9} = 7{,}9 \cdot 10^{-9}\ h^{-1}$$

Jedná se o stejné komponenty jako v případě předchozí bezpečnostní funkce, tudíž je opět u všech prvků výrobcem garantována kategorie 4 a PL = e. Vzhledem k tomu, že bezpečnostní PLC zahrnuje tři bezpečnostní výstupní moduly, je hodnota $PFH_D$ v tomto případě o něco vyšší, avšak stále dle tabulky K.1 odpovídá PL = e. Lze tedy říci, že $PL_{SB2}$ = e.

*Subsystém SB3*

$MTTF_D$ kanálu 1:

$$\frac{1}{\mathrm{MTTF_{D,SB3,k1}}} = \sum_{i=1}^{n} \frac{1}{\mathrm{MTTF_{D}}i} = 5 \cdot \frac{1}{1200} = \frac{1}{240}$$

$$\mathrm{MTTF_{D,SB3,k1}} = 240 \text{ roků}$$

$MTTF_D$ kanálu 2:

$$\frac{1}{\mathrm{MTTF_{D,SB3,k2}}} = \sum_{i=1}^{n} \frac{1}{\mathrm{MTTF_{D}}i} = 6 \cdot \frac{1}{1200} = \frac{1}{200}$$

$$\mathrm{MTTF_{D,SB3,k2}} = 200 \text{ roků}$$

$MTTF_D$ jednoho kanálu:

$$\mathrm{MTTF_D} = \frac{2}{3}\left[\mathrm{MTTF_{D,SB3,k1}} + \mathrm{MTTF_{D,SB3,k2}} - \frac{1}{\frac{1}{\mathrm{MTTF_{D,SB3,k1}}} + \frac{1}{\mathrm{MTTF_{D,SB3,k2}}}}\right]$$

$$\mathrm{MTTF_D} = \frac{2}{3}\left[240 + 200 - \frac{1}{\frac{1}{240} + \frac{1}{200}}\right]$$

$$\mathrm{MTTF_D} = 221 \text{ roků}$$

DCavg:

$$\mathrm{DC_{avg,S1}} = \frac{\frac{\mathrm{DC_1}}{\mathrm{MTTF_{D1}}} + \frac{\mathrm{DC_2}}{\mathrm{MTTF_{D2}}} + \cdots + \frac{\mathrm{DC_N}}{\mathrm{MTTF_{DN}}}}{\frac{1}{\mathrm{MTTF_{D1}}} + \frac{1}{\mathrm{MTTF_{D2}}} + \cdots + \frac{1}{\mathrm{MTTF_{DN}}}} = \frac{11 \cdot \frac{0{,}99}{1200}}{11 \cdot \frac{1}{1200}} = 0{,}99 = 99\ \%$$

Opatření proti CCF pro subsystém SB3 jsou shrnuty v tabulce č. 30.

Tab 30) Opatření proti CCF pro SB3

| **Opatření proti CCF** | **Body** |
|---|---|
| Fyzické oddělení mezi jednotlivými dráhami signálu. | 15 |
| Ochrana proti přepětí, přetlaku, nadproudu, nadteploty, atd. | 15 |
| Jsou použity osvědčené komponenty. | 5 |
| Zácvik konstruktérů za účelem pochopení příčin a následků poruch se společnou příčinou. | 5 |
| Fluidní systémy: filtrace tlakového média, zamezení nasávání nečistot, odvodnění stlačeného vzduchu, např. ve shodě s požadavky výrobce komponentu týkající se čistoty tlakového média. | 25 |
| Byly uvažovány požadavky na odolnost proti všem relevantním vlivům prostředí, např. teplota, rázy, vibrace, vlhkost (např. tak, jak je specifikováno v relevantních normách). | 10 |

Vzhledem k tomu, že $MTTF_D$ jednoho kanálu je dlouhá, $DC_{avg}$ je vysoké, požadavky týkající se opatření proti CCF byly splněny a závada v jakékoliv bezpečnostní části nevede ke ztrátě bezpečnostní funkce a je detekována při nebo před nejbližšími požadovanými bezpečnostními funkcemi, plní subsystém SB3 kritéria pro zařazení do kategorie 4. Dle tabulky K.1 normy ČSN EN ISO 13849-1 je $PFH_{D,SB3} = 1{,}08 \cdot 10^{-8}\ h^{-1}$ a $PL_{SB3} = e$.

*Celkové $PFH_{D,BF2}$ a PL*

Souhrn nejdůležitějších informací získaných od výrobce nebo výpočty pro stanovení PL funkce bezpečného zastavení pohybu beranu iniciovaná pomocí světelných závěsů je uveden v tabulce 31.

Tab 31) Shrnutí hodnot pro výpočet $PFH_D$ u BF2

| **Subsystém** | **$MTTF_D$ [roky]** | **DC [%]** | **Kat.** | **PL** | **$PFH_D$ [$h^{-1}$]** |
|---|---|---|---|---|---|
| SB1 | - | - | 4 | e | $3{,}7 \cdot 10^{-9}$ |
| SB2 | - | - | 4 | e | $7{,}9 \cdot 10^{-9}$ |
| SB3 | 221 | 99 | 4 | e | $1{,}08 \cdot 10^{-8}$ |

$$PFH_{D,BF2} = \sum_{i=1}^{n} PFH_{D,i} = 3{,}7 \cdot 10^{-9} + 7{,}9 \cdot 10^{-9} + 1{,}07 \cdot 10^{-8}$$

$$PFH_{D,BF2} = 2{,}23 \cdot 10^{-8}\ h^{-1}$$

Dle K.1 je pro $PFH_{D,BF2} = 2{,}23 \cdot 10^{-8}\ h^{-1}$ dosaženo PL = e. Všechny subsystémy mají PL = e a $PFH_{D,BF2}$ odpovídá údajům uvedeným v tabulce č. 5 této práce, tudíž $PL_{SF2}$ není nijak omezeno a je rovno e. Jsou tedy splněny požadavky na $PL_r$ = e. Ověření výsledků pomocí programu SISTEMA je součástí přílohy 3.

# 10 NÁVRH NA ZLEPŠENÍ ŘEŠENÍ FUNKČNÍ BEZPEČNOSTI V RÁMCI PROJEKTŮ

Jak vyplývá z kapitoly 8, funkční bezpečnost je v rámci působnosti brněnské firmy Bosch Rexroth řešena pouze v případě projektů, kdy jsou realizována komplexní zařízení včetně ovládacího systému. Vzhledem k tomu, že jako projekty jsou realizována různá zařízení, je nutné, aby navrhovaná řešení byla univerzální a použitelná ve všech případech. Společným znakem však je, že jejich součástí je vždy hydraulický systém. Proto je pro řešení funkční bezpečnosti nejlépe aplikovatelná norma ČSN EN ISO 13849. Navrhovaný postup by měl tedy odrážet principy a požadavky této normy.

Problematika funkční bezpečnosti a jejího zajišťování je velice obsáhlá oblast. Pro to, aby byla funkční bezpečnost zajištěna optimálním způsobem, je nutná znalost nejenom základních legislativních požadavků a norem týkajících se této problematiky, ale také praktické znalosti z mnoha technických oblastí, ať už se jedná o např. o hydraulické či elektrické systémy.

Vzhledem k tomu, že projekty nejsou realizovány pravidelně, je funkční bezpečnost aktuálně řešena externími pracovníky, protože z ekonomického hlediska je nevýhodné zaměstnávat interního specialistu. Vždy se jedná o autorizované osoby, které mají o problematice funkční bezpečnosti široký přehled a zkušenosti. Nemají však takové znalosti týkající se konkrétních technických řešení, což může být problémem pro pochopení celkové funkce zařízení, a tím i pro řešení samotné funkční bezpečnosti.

Znalostmi technických řešení nejlépe disponují samotní konstruktéři daného zařízení a další osoby podílející se na realizaci daného projektu. Každý interní pracovník se však zabývá pouze svojí oblastí a většina nemá dostatečné znalosti o funkční bezpečnosti, což je také spojeno s tím, že mnohdy nejsou externistům předány všechny důležité informace a dokumenty sloužící jako podklady pro zajištění požadované úrovně funkční bezpečnosti. Komunikace mezi interními a externími pracovníky může tedy být komplikovaná a časově náročná.

Řešením je poskytnout daným pracovníkům potřebné informace týkající se zajišťování funkční bezpečnosti ve formě školení. Pro tyto účely byla vytvořena prezentace popisující vztah mezi celkovou bezpečností produktu a funkční bezpečností, dále základní pojmy a normy z oblasti funkční bezpečnosti a postup pro zajištění funkční bezpečnosti. Školení proběhlo v několika termínech v průběhu května. Připraveny byly dvě verze. První verze (základní) byla určena primárně pro pracovníky prodeje, u nichž je nutná alespoň základní znalost problematiky, aby mohli diskutovat se zákazníky jejich požadavky, odhadnout náklady na zajištění bezpečnosti atd. Druhá verze školení (technická) byla více zaměřena na návrh bezpečnostních funkcí včetně stručné ukázky na konkrétním příkladu. Cílovou skupinou byli hlavně pracovníci aplikačního inženýrignu, konstrukce a další, kteří se podílí na návrhu zařízení.

Kvalitním školením lze docílit toho, aby byla funkční bezpečnost v budoucnosti řešena primárně interně. V rámci každého projektu by byl sestaven tým, který by se zabýval touto problematikou, přičemž u složitějších projektů by bylo možné využít spolupráci s externími pracovníky ve formě konzultací. Nemělo by však být po externistech vyžadováno komplexní řešení funkční bezpečnosti, protože jejich znalosti z pohledu daného produktu mohou být nedostačující.

Díky tomu, že by komunikace probíhala převážně interně, by bylo možné výrazně snížit časovou náročnost řešení. Další výhodou by také bylo snížení nákladů na realizaci projektů, čímž by mohla být zvýšena jejich ziskovost.

Zkrácení doby potřebné pro řešení funkční bezpečnosti však souvisí také s tím, že je nutné, aby byly včas k dispozici všechny relevantní vstupní materiály a informace. Obecně pro zajištění, že jsou v dané fázi projektu k dispozici potřebné dokumenty a podklady, jsou využívány tzv. Quality Gates (QG). Jedná se o 5 milníků, které umístěny vždy na konci daných fází projektu, a to od nabídkové fáze až po uvedení do provozu. Každá QG obsahuje body, jež musí být v jednotlivých fázích projektu splněny, aby bylo možné postoupit do další fáze. Při správném využívání tohoto nástroje lze včas odhalit problémy spojené s realizací projektu a odchylky od definovaných cílů. QG lze chápat také jako návod pro postup při realizaci projektů.

Z pohledu zajištění funkční bezpečnosti je ale jejich obsah nedostačující. Součástí jednotlivých QG je pouze několik bodů, které souvisí spíše obecně s bezpečností produktu. Může se tedy stát, že funkční bezpečnost, ačkoliv je součástí celkové bezpečnosti, bude úplně opomenuta, a nebudou tak splněny všechny relevantní legislativní požadavky. S tím opět souvisí již zmíněný fakt, že spousta pracovníků nemá o důležitosti funkční bezpečnosti dostatečné povědomí. Mimo to jsou některé body nevhodně zařazeny do daných QG. Jedná se např. o dokončení posouzení rizik, které je v současné době umístěné v QG3, tzn. ve fázi, kdy je řešen konstrukční návrh zařízení. Posouzení rizik by mělo být dokončeno už před finalizací návrhu systému, protože již samotný návrh systému musí být vytvořen tak, aby konečné zařízení bylo bezpečné a představovalo pro uživatele minimální riziko. Vzhledem k tomu, že posouzení rizik je velice důležitým dokumentem pro zajištění požadované úrovně funkční bezpečnosti, je nutné, aby tomu odpovídala také kvalita jeho zpracování. Pro zajištění tohoto požadavku byla navržena jednotná šablona (viz příloha 1), která odráží požadavky normy ČSN EN ISO 12100. Tato šablona byla využita při řešení reálného projektu v kapitole 9 a bude dále aktivně využívána i u dalších projektů.

Tabulka č. 31 uvádí porovnání současného stavu a návrhu, jakým způsobem by měl být obsah jednotlivých QG upraven. Navrhované úpravy vychází z teoretických znalostí uvedených v kapitole 5.3 a jejich aplikace na konkrétní projekt v kapitole 9.

Se zajištěním potřebných podkladů je spojeno také vynechávání některých QG v závislosti na kategorii projektu. Tento případ nastává u projektů kategorie D1 a D2, které jsou z pohledu náročnosti nejjednodušší, a obsah vynechaných QG je považován za nerelevantní. Vzhledem k tomu, že vynechané QG obsahují body, které souvisí se zajištěním bezpečnosti produktu a jejich splnění nebude nikterak ověřeno, může se stát, že nebudou k dispozici všechny podklady a informace potřebné pro realizaci dalších fází projektu nebo v horším případě nebude odhaleno opomenutí legislativních požadavků či požadavků zákazníka. To se týká obzvláště QG2, protože z návrhu v tabulce č. 31 je patrné, že největší část při řešení funkční bezpečnosti je realizována právě ve fázi návrhu systému, která je zakončena touto QG. Z pohledu bezpečnosti by měly mít všechny QG stejnou váhu, protože opomenutí a nesplnění bezpečnostních požadavků může vážně ohrozit zdraví osob bez ohledu na kategorii projektu. Je pochopitelné, že v případě jednodušších projektů nejsou všechny body obsažené ve vynechaných QG relevantní, avšak zajištění bezpečnosti produktu je nutné vždy. Řešením by tedy bylo nevynechávat definované QG, ale realizovat je alespoň v podobě zjednodušené verze, která by obsahovala pouze body týkající se bezpečnosti produktu.

Tab 32) Porovnání současného stavu a návrhu na úpravu bodů relevantních pro funkční bezpečnost v jednotlivých QG

| | **Současný stav** | **Návrh na zlepšení** |
|---|---|---|
| **QG1** | ✓ ověření technických požadavků (dostupnost, legálnost a proveditelnost),<br>✓ zahájení posouzení rizik,<br>✓ vytvoření základního návrhu systému,<br>✓ zahrnutí nákladů spojených se zajištěním požadované úrovně bezpečnosti do celkové kalkulace. | ✓ ověření technických požadavků (dostupnost, legálnost a proveditelnost),<br>✓ vytvoření seznamu aktuálních předpisů a norem relevantních pro daný produkt,<br>✓ zvážení relevantnosti CE prohlášení o shodě,<br>✓ vytvoření předběžného posouzení rizik zahrnující definici základních opatření pro snížení významných rizik (např. na základě norem typu C),<br>✓ identifikace klíčových bezpečnostních funkcí, stanovení jejich $PL_r$ a volba kategorie (např. s využitím norem typu C),<br>✓ vytvoření návrhu systému,<br>✓ zahrnutí nákladů spojených se zajištěním požadované úrovně bezpečnosti do celkové kalkulace. |
| **QG2** | ✓ dokončení návrhu systému,<br>✓ vytvoření kusovníku,<br>✓ zvážení relevantnosti CE prohlášení o shodě,<br>✓ schválení konečného návrhu. | ✓ vypracování kompletního posouzení rizik a případně definice dalších bezpečnostních funkcí, stanovení jejich $PL_r$ a volba kategorie, pokud nebyly v rámci QG1 identifikovány všechny bezpečnostní funkce,<br>✓ dokončení návrhu systému (hydraulická a elektrická schémata),<br>✓ vytvoření kusovníku,<br>✓ návrh bezpečnostních funkcí (sestavení bezpečnostních blokových schémat),<br>✓ zjištění hodnot potřebných pro stanovení PL ($MTTF_D$, $B_{10D}$,…),<br>✓ odhad PL a ověření, zda $PL \geq PL_r$,<br>✓ v případě, že $PL < PL_r$, navrhnutí úprav, opětovný odhad PL a změna relevantní dokumentace dle nového návrhu (hydraulická a elektrická schémata, kusovník atd.)<br>✓ návrh software (v případě, že je relevantní),<br>✓ vytvoření plánu ověření platnosti,<br>✓ ověření platnosti,<br>✓ schválení konečného návrhu systému. |
| **QG3** | ✓ dokončení posouzení rizik,<br>✓ zahájení vytváření návodů pro uživatele. | ✓ zahájení vytváření návodů pro uživatele. |

| | | |
|---|---|---|
| **QG4** | ✓ ověření implementace všech opatření vycházejících<br>✓ z posouzení rizik,<br>✓ zahájení zpracování CE prohlášení o shodě v případě, že je relevantní. | ✓ realizace bezpečnostních funkcí,<br>✓ ověření implementace všech opatření vycházejících z posouzení rizik,<br>✓ zahájení zpracování CE prohlášení o shodě v případě, že je relevantní. |
| **QG5** | ✓ dokončení návodů k zařízení. | ✓ ověření platnosti,<br>✓ dokončení návodů k zařízení. |

Vzhledem k již zmíněnému faktu, že funkční bezpečnost v rámci projektů byla doposud řešena externími pracovníky, neexistují ani interní dokumenty, které by popisovaly zajišťování funkční bezpečnosti v prostředí brněnské společnosti Bosch Rexroth. Z tohoto důvodu by tedy bylo vhodné z poznatků získaných nejenom na základě této závěrečné práce, ale také na základě informací získaných od dalších závodů Bosch Rexroth, vytvořit dokument, který by objasňoval podrobněji celý proces zajištění funkční bezpečnosti, včetně reálných příkladů. Součástí by byly také tzv. „Q-basics“ pro funkční bezpečnost, které byly představeny i v rámci již zmiňovaného školení. Jedná se o souhrn nejzásadnějších poznatků a informací důležitých pro řešení funkční bezpečnosti v prostředí společnosti.

# 11 ZÁVĚR

Hlavním cílem diplomové práce bylo navrhnout zlepšení procesů zajišťování funkční bezpečnosti v brněnské firmě Bosch Rexroth se zaměřením na řešení projektů.

Nejprve bylo nutné se zabývat základními legislativními předpisy, které stanovují požadavky související obecně s bezpečností produktů. V úvodní části byly tedy představeny nejdůležitější předpisy vydané Evropskou unií a zákony České republiky, které je přebírají. Zvláštní pozornost byla věnována směrnici Evropského parlamentu a Rady 2006/42/ES stanovující obecné požadavky na bezpečnost strojních zařízení, jež je vzhledem k zaměření společnosti stěžejním dokumentem. S touto směrnicí také úzce souvisí harmonizované normy, jejichž cílem je usnadnit plnění uvedených požadavků v praxi. Kromě obecného pojednání o harmonizovaných normách zde byly také popsány jednotlivé normy potřebné pro splnění cílů této práce. Jednalo se o normu ČSN EN ISO 12100 zabývající se posouzením rizik, která je základem pro zajištění bezpečnosti strojních zařízení, dále také o normy zaměřené na funkční bezpečnost ČSN EN 61508, ČSN EN ISO 13849 a ČSN EN 62061 a o normu ISO 16092 věnující se bezpečnosti lisů.

Dále byla popsána společnost Bosch Rexroth Brno vyrábějící hydraulické systémy a prodávající komponenty vyráběné ostatními závody Bosch Rexroth po celém světě. Produktové portfolio zahrnuje hydraulické komponenty, hydraulické agregáty a projekty a u každé z oblastí bylo objasněno, jakým způsobem je funkční bezpečnost zajišťována. U komponent není funkční bezpečnost brněnskou pobočkou řešena, protože zde nejsou komponenty vyráběny, ale pouze prodávány. Odpovědný je tedy daný výrobní závod. V případě hydraulických agregátů, kdy se jedná o neúplná strojní zařízení, odpovídá za funkční bezpečnost konečný výrobce, protože způsob zapojení agregátu do celku může mít zásadní vliv na výslednou bezpečnost celého zařízení. Poslední oblastí jsou projekty, v rámci nichž jsou již řešena komplexní zařízení včetně ovládacího systému. Jedná se tedy o jedinou oblast, kde je funkční bezpečnost aktivně řešena. Aktuálně je u většiny projektů využívána spolupráce s externími autorizovanými pracovníky.

Důležitou částí pro splnění hlavního cíle bylo popsat současný stav v oblasti projektového řízení ve společnosti. Projekty jsou řešeny v sedmi fázích: od akvizice až po uzavření projektu. Součástí pěti fází jsou tzv. Quality Gates (QG) umístěné vždy na konci fáze. Jedná se o nástroj, jehož cílem je zajistit, že budou k dispozici všechny potřebné podklady a informace pro realizaci další fáze. QG jsou řešeny formou check-listů, kde jsou uvedeny všechny podstatné činnosti v podobě bodů. Součástí jsou mimo jiné také body týkající se funkční bezpečnosti.

Jedním z projektů, který byl řešen v průběhu roku 2019/2020 byl zapracovávací (zkušební) lis MW 2100, který je využíván k odzkoušení nástrojů určených pro tvarování dílů karoserií automobilů před jejich instalací v sériové výrobě. Na tomto projektu byl objasněn postup řešení funkční bezpečnosti.

Základem je vždy vypracování posouzení rizik. To bylo zpracováno pro vybranou část životního cyklu zařízení – provoz. V rámci toho byla navržena univerzálně použitelná šablona respektující požadavky uvedené v normě ČSN EN ISO 12100, která může zaměstnancům posloužit také jako návod. Následně byly vybrány dvě bezpečnostní funkce, které se podílejí na snížení rizik spojených s provozem lisu.

Jednalo se o funkci nouzového zastavení realizovanou odpojením hlavních stykačů a funkci bezpečného zastavení pohybu beranu iniciovanou pomocí světelných závěsů. Obě funkce byly popsány včetně požadavků dle ČSN EN ISO 16092-3, dále byla pomocí elektrických a hydraulických schémat navržena bloková schémata a bylo odhadnuto PL. Navrhované funkce splnily požadovanou úroveň funkční bezpečnosti.

Na základě informací zjištěných v jednotlivých částech této práce bylo identifikováno několik nedostatků:

- Pro řešení funkční bezpečnosti jsou využíváni externí pracovníci, kteří nemusejí mít dostatečné znalosti technického řešení systému pro správné pochopení celkové funkce daného zařízení, což může ovlivnit i samotné řešení funkční bezpečnosti.
- Interní pracovníci nemají dostatečné znalosti týkající se funkční bezpečnosti a jejího zajišťování.
- Obsah jednotlivých Quality Gates je nedostačující.
- Některé Quality Gates jsou v závislosti na kategorii projektu vynechávány.

Pro eliminaci zmíněných nedostatků bylo navrženo několik zlepšení. Prvním z nich bylo seznámení zaměstnanců s problematikou funkční bezpečnosti. Školení proběhlo ve dvou verzích (základní a technická). Pro zaměstnance z oddělení prodeje a aplikačního inženýringu bylo povinné, ostatní zaměstnanci se mohli zúčastnit dobrovolně. I přes to, že pro většinu bylo školení dobrovolné, zúčastnila se více než polovina zaměstnanců, takže lze vidět zájem o danou problematiku a ochotu učit se novým věcem. Alespoň základní znalost problematiky může výrazně zjednodušit a urychlit komunikaci mezi interními pracovníky a externisty či zákazníky. Do budoucna by také mohlo být docíleno toho, aby funkční bezpečnost byla standardně řešena interními zaměstnanci, kteří se podílejí na návrhu daného zařízení, čímž by byly sníženy náklady spojené se zajištěním externích služeb.

Pro to, aby byla funkční bezpečnost řešena interními pracovníky, by bylo také vhodné vytvořit dokument popisující zajišťování funkční bezpečnosti v prostředí společnosti, který by sloužil zaměstnancům jako hlavní zdroj informací a návod. Aktuálně tento dokument alespoň částečně nahrazují podklady ze školení, kde jsou také mimo jiné uvedeny tzv. Q-basic pro funkční bezpečnost, jež shrnují nejdůležitější zásady potřebné pro řešení funkční bezpečnosti.

Dále byla navržena úprava QG, které aktuálně obsahují spíše body týkající se obecně produktové bezpečnosti bez důrazu na nutnost zabývat se také funkční bezpečností. Rovněž jsou některé body zařazeny do jednotlivých QG nevhodně. Do stávajících QG byly tedy doplněny body týkající se zajištění funkční bezpečnosti a již uvedené body, které byly nevhodně umístěny, byly přesunuty. Vznikla tak obohacenější verze QG, kterou lze využívat jako návod popisující jednotlivé kroky potřebné pro zajištění funkční bezpečnosti zařízení. Pro lepší názornost byly také v rámci školení funkční bezpečnosti představeny jednotlivé kroky navázané na fáze projektu v grafické podobě.

Realizace jednotlivých QG by také neměla záviset na kategorizaci projektu. Ačkoliv obecně některé body nemusejí být pro projekty nižších kategorií relevantní, bezpečnost produktů je nutné řešit vždy. Vynecháním některý QG se může stát, že budou některé důležité body opomenuty, což může v nejhorším případě vést až ke škodě na zdraví. Bylo by tedy vhodné realizovat všechny QG alespoň ve zjednodušené formě, která by obsahovala body týkající se bezpečnosti produktů.

Problematika funkční bezpečnosti je v rámci společnosti již delší dobu diskutovaným tématem a jedná se o oblast s velkým potenciálem pro zlepšování, která nebyla doposud takto komplexně řešena, proto lze práci hodnotit jako přínosnou. Do budoucna by bylo vhodné zpracovat také postup pro zajištění funkční bezpečnosti u softwaru a doplnit QG o další body s tímto spojené.

# 12 SEZNAM POUŽITÝCH ZDROJŮ

[1] EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE. *Směrnice Evropského parlamentu a Rady 2001/95/ES ze dne 3. prosince 2001 o obecné bezpečnosti výrobků*. In: Úřední věstník Evropské unie, 2002, L 11, s. 4—17. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1587031271709&uri=CELEX:32001L0095

[2] EVROPSKÁ KOMISE. *„Modrá příručka" k provádění pravidel EU pro výrobky 2016*. In: Úřední věstník Evropské unie, 2016, C272, s. 1—149. ISSN 1977-0863. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.C_.2016.272.01.0001.01.CES&toc=OJ:C:2016:272:FULL

[3] ČESKO. Zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 2020-11-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/1997-22/zneni-20170901

[4] ČESKO. Zákon č. 90/2016 Sb., o posuzování shody stanovených výrobků při jejich dodávání na trh. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 2020-11-26]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-90/zneni-20180612

[5] EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE. *Směrnice Evropského parlamentu a Rady 2006/42/ES ze dne 17. května 2006 o strojních zařízeních a o změně směrnice 95/16/ES*. In: Úřední věstník Evropské unie, 2006, L 157, s. 24—86. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1587031893336&uri=CELEX:32006L0042

[6] ČSN EN ISO 12100. *Bezpečnost strojních zařízení – Všeobecné zásady pro konstrukci – Posouzení rizika a snižování rizika*. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011, 106 s.

[7] BARG, Jürgen, Franz EISENHUT-FUCHSBERGER, Alexandre ORTH, Jochen OST a Carsten SPRINGHORN. *10 steps to performance level: Handbook for the implementation of functional safety according to ISO 13849*. Germany: Bosch Rexroth, 2012. ISBN 978-3-9814879-2-3.

[8] Funkční bezpečnost - pro mnoho výrobců stále ještě velká neznámá. *MM Průmyslové spektrum* [online]. 2002, **2002**(9), 102 [cit. 2020-12-01]. Dostupné z: https://www.mmspektrum.com/clanek/funkcni-bezpecnost-pro-mnoho-vyrobcu-stale-jeste-velka-neznama.html

[9] ČSN EN 61508-1 ED. 2. *Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností - Část 1: Všeobecné požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011., 60 s.

[10] ČSN EN 61508-4 ED. 2. *Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností - Část 4: Definice a zkratky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011, 36 s.

[11] UHER, Jaromír. Úvod do funkční bezpečnosti I: norma ČSN EN 61508. *Automa: Časopis pro automatizační techniku* [online]. **2004**(08) [cit. 2020-01-18]. Dostupné z: https://automa.cz/cz/casopis-clanky/uvod-do-funkcni-bezpecnosti-i-norma-csn-en-61508-2004_08_32520_3609/

[12] ČSN EN 61508-5 ED. 2. *Funkční bezpečnost elektrických / elektronických / programovatelných elektronických systémů souvisejících s bezpečností - Část 5: Příklady metod určování úrovní integrity bezpečnosti*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011, 56 s.

[13] ČSN EN ISO 13849-1. *Bezpečnost strojních zařízení - Bezpečnostní části ovládacích systémů - Část 1: Obecné zásady pro konstrukci*. 3. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017, 88 s.

[14] ČSN EN ISO 13849-2. *Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 2: Ověřování platnosti*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[15] ČSN EN 62061. *Bezpečnost strojních zařízení – Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností*. Praha: Český normalizační institut, 2005, 92 s.

[16] ISO/TR 23849. *Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery*. Switzerland: International Organization for Standardization, 2010, 14 s.

[17] ČSN EN ISO 16092-1. Bezpečnost obráběcích a tvářecích strojů – Lisy – Část 1: Obecné bezpečnostní požadavky. Praha: Česká agentura pro standardizaci, 2019, 76 s.

[18] ČSN EN ISO 16092-3. Bezpečnost obráběcích a tvářecích strojů – Lisy – Část 3: Bezpečnostní požadavky pro hydraulické lisy. Praha: Česká agentura pro standardizaci, 2019, 76 s.

[19] ZVOLÁNKOVÁ, K. *Rozvoj procesu neustálého zlepšování v obchodně-výrobní společnosti*, Brno, Vysoké učení technické v Brně, Fakulta strojního inženýrství. 2018, 88 s., Vedoucí bakalářské práce doc. Ing. Petr Blecha, Ph.D.

[20] AIDAnova Theatrium. In: *Alex Travel* [online]. [cit. 2020-01-15]. Dostupné z: https://www.alextravel.at/kreuzfahrt-kanaren-mit-aida-nova/aidanova_theatrium_kreuzfahrt-gran-canaria_alex-travel/

[21] Rexroth Safety on Board - Your path to intelligent and economical machine safety. *Rexroth: A Bosch Company* [online]. Bosch Rexroth [cit. 2020-01-18]. Dostupné z: https://www.boschrexroth.com/en/xc/trends-and-topics/machine-safety/machine-safety

[22] CANO, Nicolas. *Press Module IH04 Type C*. Lohr am Maim, 2017.

[23] MÜHLENBRUCH, Andreas. BOSCH REXROTH AG. *DCCS 06001-10 Principles on the Product Safety of Hydraulic Power Units: General requirements, definitions and master approach*. Lohr a. Main, 2015, 15 s.

[24] BUTZ, Dieter. ROBERT BOSCH GMBH. *CD 02500 Project Management at Bosch*. Germany, 2019, 23 s.

[25] BOSCH REXROTH AG. *DCCD 08924 Project Management at Bosch: DC specific regulations/supplements*. Lohr a. Main, 2019, 5 s.

[26] BOSCH REXROTH B. V. DCGP 18344-006: Project Business Process Landscape: Stepwise approach to project execution process landscape. Netherlands, 2018, 38 s.

[27] BOSCH REXROTH AG. *DCCD 08934 Quality Gates (QG)*. Lohr a. Main, 2019, 10 s.

[28] BOSCH REXROTH B. V. *DCFR 18344-006 Project Quality Assessment Tool*. Netherlands, 2020.

[29] BOSCH REXROTH B. V. DCFR 07924-005 Project Category Tool. Netherlands, 2019.

[30] Hydraulic press / tryout / for the automotive industry. In: *Direct industry* [online]. [cit. 2020-02-21]. Dostupné z: https://www.directindustry.com/prod/schuler-mueller-weingarten/product-13229-919551.html

[31] ISO/TR 14121-2. *Safety of machinery - Risk assessment - Part2: Practical guidance and examples of methods*. 2nd edition. Switzerland: International Organization for Standardization, 2012, 38 s.

[32] ČSN EN ISO 13850. *Bezpečnost strojních zařízení – Funkce nouzového zastavení – Zásady pro konstrukci*. 3. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017, 20 s.

[33] Power Units. In: *Rexroth: A Bosch Company* [online]. Bosch Rexroth [cit. 2020-05-18]. Dostupné z: https://www.boschrexroth.com/en/xc/products/product-groups/industrial-hydraulics/topics/power-units/index

# 13 SEZNAM TABULEK A OBRÁZKŮ

## 13.1 Seznam tabulek

## 13.2 Seznam obrázků

# 14 SEZNAM ZKRATEK A SYMBOLŮ

| | |
|---|---|
| AG | Aktiengesellschaft (akciová společnost) |
| ALARP | As Low As Reasonable Practicable (nejmenší rozumně použitelný) |
| AOPD | Active Opto-electronic Protective Device (aktivní optoelektronické ochranné zařízení) |
| $B_{10}$ | Střední počet cyklů do výpadku 10 % komponent |
| $B_{10D}$ | Počet cyklů do 10 % nebezpečných selhání komponentů |
| c | Křížové monitorování |
| CCF | Common Cause Failure (porucha se společnou příčinou) |
| CD | Central Directive (centrální směrnice) |
| CI | Třída pravděpodobnosti škody |
| CPU | Central Processing Unit (centrální procesorová jednotka - procesor) |
| ČR | Česká republika |
| ČSN | Česká technická norma |
| DC | Diagnostic Coverage (diagnostické pokrytí) |
| $DC_{avg}$ | Average diagnostic coverage (průměrné diagnostické pokrytí) |
| DCCD | Drives and Control Central Directive (centrální pokyny pro oblast průmyslové automatizace) |
| DCCS | Drives and Control Central Standard (závodní norma pro oblast průmyslové automatice) |
| $d_{op}$ | Střední doba provozu ve dnech za rok |
| E/E/PE | Elektrický / elektronický / programovatelný elektronický |
| EN | Evropská norma |
| ES | Evropské společenství |
| EU | Evropská unie |
| $h_{op}$ | Střední doba provozu v hodinách za den |
| I | Vstupní zařízení |
| $i_m$ | Prostředky vzájemného propojení |
| ISO | International Organization for Standardization (Mezinárodní organizace pro normalizaci) |
| IT | Informační Technologie |
| L | Logika |
| LED | Light Emitting Diode (světlo vyzařující dioda) |
| LOPA | Layer of protection analysis (analýza vrstev ochrany) |
| m | Monitorování |

| | |
|---|---|
| $MTTF_D$ | Mean Time to Dangerous Failure (střední doba do nebezpečné poruchy) |
| NC | Normally Closed (rozpínací kontakt) |
| $n_{op}$ | Střední počet ročního provozu |
| O | Výstupní zařízení |
| OM | Other Measure (jiné opatření) |
| OSSD | Output Signal Switching Device (výstupní spínací prvek) |
| OTE | Výstup ze zkušebního zařízení |
| $PFD_{avg}$ | Průměrná pravděpodobnost nebezpečné chyby na vyžádání |
| PFH | Průměrná pravděpodobnost nebezpečné chyby za hodinu |
| $PFH_D$ | Průměrná pravděpodobnost nebezpečné poruchy za hodinu |
| PL | Performance Level (úroveň vlastností) |
| PLC | Programmable Logic Controller (programovatelná logická řídicí jednotka) |
| $PL_r$ | Required Performance Level (požadovaná úroveň vlastností) |
| QG | Quality Gate |
| RAPEX | Rapid Alert System for Non-Food Products (rychlý výstražný informační systém Evropské unie o nebezpečných spotřebitelských výrobcích nepotravinářského charakteru) |
| spol. s r.o. | Společnost s ručením omezeným |
| Sb. | Sbírka zákonů |
| SDI | Safety Digital Input (bezpečnostní vstupní modul) |
| SDO | Safety Digital Output (bezpečnostní výstupní modul) |
| SIL | Safety Integrity Level (úroveň integrity bezpečnosti) |
| SISTEMA | Safety Integrity Software Tool for the Evaluation of Machine Applications |
| SRCF | Safety-Related Control Function (řidící funkce související s bezpečností) |
| SRECS | Safety-Related Electrical Control System (elektrický řídicí systém související s bezpečností) |
| SRP/CS | Safety-Related Part of a Control System (bezpečnostní část ovládacího systému) |
| SW | Software |
| $t_{cyklu}$ | Střední doba mezi začátkem dvou po sobě následujících cyklů komponentu |
| TE | Zkušební zařízení |
| TR | Technical Report (technická zpráva) |

# 15 SEZNAM PŘÍLOH

Příloha 1: Posouzení a snížení rizik

Příloha 2: Odhad PL pomocí softwaru SISTEMA_BF1

Příloha 3: Odhad PL pomocí softwaru SISTEMA_BF2